**Sobre a quantidade de curvas elípticas satisfazendo a
conjectura de Birch e Swinnerton-Dyer**

Eduardo Rocha Walchek

Dissertação de Mestrado do Programa de Pós-Graduação em
Matemática (PPG-Mat)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Eduardo Rocha Walchek

Sobre a quantidade de curvas elípticas satisfazendo a conjectura de Birch e Swinnerton-Dyer

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Matemática. *VERSÃO REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Junho de 2020

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

W154s Walchek, Eduardo Rocha
Sobre a quantidade de curvas elípticas
satisfazendo a conjectura de Birch e Swinnerton-
Dyer / Eduardo Rocha Walchek; orientador Herivelto
Martins Borges Filho. -- São Carlos, 2020.
167 p.

Dissertação (Mestrado - Programa de Pós-Graduação
em Matemática) -- Instituto de Ciências Matemáticas
e de Computação, Universidade de São Paulo, 2020.

1. Curvas elípticas. 2. Conjectura de Birch e
Swinnerton-Dyer. 3. Grupos de Selmer. 4. Grupo de
Tate--Shafarevich. I. Borges Filho, Herivelto
Martins, orient. II. Título.

Eduardo Rocha Walchek

**On the quantity of elliptic curves satisfying the Birch and
Swinnerton-Dyer conjecture**

Dissertation submitted to the Institute of Mathematics
and Computer Sciences – ICMC-USP – in accordance
with the requirements of the Mathematics Graduate
Program, for the degree of Master in Science. *FINAL
VERSION*

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
June 2020

À minha família.

AGRADECIMENTOS

Ao professor Herivelto Borges, que teve paciência em me orientar desde minha iniciação científica até o mestrado, e ao professor Eduardo Tengan, que me apresentou ao mundo das curvas elípticas.

Ao Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo, onde adquiri indispensável e sólida formação, tanto pelos excelentes professores que tive, quanto pelo ambiente propício à pesquisa e ao estudo.

Aos professores Daniel Levcovitz e Victor Neumann, pelos comentários, correções e sugestões para o melhoramento desta obra.

Este trabalho foi realizado com o auxílio imprescindível da Fundação de Amparo à Pesquisa do Estado de São Paulo (processo 2019/07386-8), à qual sou imensamente grato.

*“[...] mi perdoni s’io son statto troppo longo
ma incolpi la mia ignoranza che non mi ha
lassiato imparare a dir conciso [...]”*

(Claudio Monteverdi, em carta a Alessandro Striggio, filho, em 10 de Setembro de 1609)

RESUMO

WALCHEK, E. R. **Sobre a quantidade de curvas elípticas satisfazendo a conjectura de Birch e Swinnerton-Dyer.** 2020. 167 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

Neste trabalho, estudamos propriedades de curvas elípticas sobre $\mathbb{Q}$, seus grupos de Tate–Shafarevich e grupos de Selmer, com vistas a um resultado de [Bhargava, Skinner e Zhang \(2014, p. 1, Teorema 1\)](#) que afirma que a maioria (mais de 66 por cento) de tais curvas elípticas, quando ordenadas por altura, satisfazem a conjectura de Birch e Swinnerton-Dyer, um dos principais problemas em aberto da Teoria dos Números moderna.

Palavras-chave: Curvas elípticas, Conjectura de Birch e Swinnerton-Dyer, Grupos de Selmer, Grupo de Tate–Shafarevich.

ABSTRACT

WALCHEK, E. R. **On the quantity of elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture**. 2020. 167 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

In this work, we studied properties of elliptic curves over $\mathbb{Q}$, their associated Tate–Shafarevich groups and Selmer groups, with an eye towards a result by [Bhargava, Skinner e Zhang \(2014, p. 1, Theorem 1\)](#) which states that the majority (over 66 percent) of such elliptic curves, when ordered by height, satisfies the Birch and Swinnerton-Dyer conjecture, one of the main open problems in modern Number Theory.

Keywords: Elliptic curves, Birch and Swinnerton-Dyer conjecture, Selmer groups, Tate–Shafarevich group.

SUMÁRIO

INTRODUÇÃO	19
1 PRELIMINARES	23
1.1 Tópicos de curvas algébricas	23
1.1.1 <i>Variedades algébricas</i>	23
1.1.2 <i>Propriedades específicas de curvas algébricas</i>	26
1.1.3 <i>Mapas entre variedades algébricas</i>	27
1.1.4 <i>Gênero e o teorema de Riemann–Roch</i>	29
1.1.5 <i>Curvas algébricas sobre corpos finitos</i>	29
1.2 Tópicos de co-homologia de Galois	30
1.2.1 <i>Co-homologia de Galois e isomorfismos de curvas algébricas</i>	33
1.3 Tópicos de grupos abelianos divisíveis	33
1.4 Tópicos de valorizações	35
1.4.1 <i>Extensões de valorizações</i>	37
1.4.2 <i>Completamento de corpos de valorizações</i>	38
1.5 Tópicos de números p -ádicos	39
1.5.1 <i>Uma decomposição útil</i>	40
1.5.2 <i>Logaritmo p-ádico</i>	41
1.5.3 <i>Estendendo a norma p-ádica</i>	42
1.6 Tópicos de Teoria Algébrica dos Números	42
1.6.1 <i>Extensões de ideais primos</i>	43
1.6.2 <i>Elementos de Frobenius</i>	44
1.6.3 <i>Lugares em corpos de números</i>	45
1.7 Tópicos de formas modulares	46
1.7.1 <i>Operadores de Hecke</i>	50
1.7.1.1 <i>Caracteres</i>	51
1.7.1.2 <i>Autoformas de Hecke</i>	52
1.8 Tópicos de L -funções	53
2 CURVAS ELÍPTICAS	57
2.1 Cúbicas de Weierstrass e curvas elípticas	57
2.2 Redução de curvas elípticas módulo valorizações	64
2.3 Curvas elípticas sobre $\mathbb{C}$	67

2.3.1	<i>Toros complexos</i>	68
2.3.2	<i>Curvas elípticas complexas são toros</i>	69
2.4	Curvas elípticas sobre $\mathbb{Q}_p$	70
2.4.1	<i>Curva de Tate</i>	73
2.4.2	<i>Curvas elípticas p-ádicas são “toros”</i>	74
2.4.3	<i>Invariante de Mazur–Tate–Teitelbaum</i>	75
3	CURVAS ELÍPTICAS SOBRE $\mathbb{Q}$	77
3.1	O Teorema de Mordell–Weil e o posto algébrico	77
3.1.1	<i>Observações sobre a prova do Teorema de Mordell–Weil</i>	79
3.2	L -funções e o posto analítico	81
3.2.1	<i>Critérios para distinguir os tipos de redução boa</i>	83
3.3	A Conjectura de Birch e Swinnerton-Dyer	85
3.3.1	<i>Computando o grupo de uma curva elíptica</i>	85
3.3.1.1	<i>Computando o subgrupo de torção</i>	86
3.3.1.2	<i>Computando o posto algébrico</i>	87
3.3.1.3	<i>Computando os geradores de $E(\mathbb{Q})$</i>	88
3.4	Representações de Galois	89
3.4.1	<i>Representações de Galois Residuais</i>	90
4	GRUPOS DE SELMER E GRUPOS DE TATE–SHAFAREVICH	93
4.1	Espaços homogêneos e grupos de Weil–Châtelet	93
4.2	Sequências de Kummer	97
4.3	Grupos de Selmer e grupos de Tate–Shafarevich	99
4.3.1	<i>Finitude dos grupos de Selmer</i>	101
4.3.2	<i>Finitude do grupo de Tate–Shafarevich</i>	105
4.3.3	<i>A p-descida e o posto algébrico</i>	107
4.3.4	<i>A p^∞-descida e o posto algébrico</i>	108
5	QUANTAS CURVAS ELÍPTICAS SATISFAZEM A CONJECTURA DE BIRCH E SWINNERTON-DYER?	115
5.1	Contando curvas elípticas sobre $\mathbb{Q}$	117
5.1.1	<i>Famílias de curvas elípticas</i>	118
5.1.2	<i>Root numbers</i>	120
5.1.3	<i>O posto algébrico médio</i>	122
5.2	A estratégia da prova	123
5.3	Três teoremas importantes	124
5.3.1	<i>As condições sobre os p-grupos de Selmer</i>	128
5.4	A maioria das curvas elípticas satisfaz BSD	133
5.4.1	<i>Quanto é “a maioria”?</i>	142

REFERÊNCIAS	145
APÊNDICE A MAIS SOBRE A CONJECTURA BSD	155
A.1 A conjectura forte de Birch e Swinnerton-Dyer	155
A.1.1 <i>Regulador elíptico</i>	155
A.1.2 <i>Números de Tamagawa</i>	157
A.1.3 <i>Período real</i>	157
A.1.3.1 <i>Componentes conexas de uma curva elíptica sobre $\mathbb{R}$</i>	157
A.1.3.2 <i>Definição do período real</i>	159
A.1.4 <i>A conjectura</i>	160
A.2 Outras aplicações da conjectura BSD	163
A.2.1 <i>Problema do número congruente</i>	163
A.2.2 <i>Primos que são somas de dois cubos racionais</i>	165
A.3 Linha do tempo da conjectura BSD	166

INTRODUÇÃO

Grosso modo, as curvas elípticas são objetos de dupla natureza: por um lado, são curvas algébricas planas não-singulares, e por outro, são grupos abelianos. Particularmente para as curvas elípticas sobre $\mathbb{Q}$, sabe-se que tais grupos abelianos são finitamente gerados (Teorema de Mordell–Weil, 3.1.1) e até mesmo se conhece exatamente a parte de torção (Teorema de Mazur, 3.1.2), mas pouco se sabe sobre o **posto algébrico**, isto é, o tamanho da parte livre. Não se sabe que valores este número pode atingir, nem quão grande pode chegar a ser.

Todas as técnicas conhecidas para se calcular posto algébrico dependem do problema de se determinar **pontos $\mathbb{Q}$ -racionais** em uma curva elíptica, que é um problema difícil em geral, mas para quase toda curva algébrica - exceto para as curvas elípticas! - podemos pelo menos dizer se existem finitos ou infinitos destes pontos. Infinitos pontos significam posto algébrico positivo. Finitos pontos significam posto algébrico nulo. A dificuldade em determinar pontos racionais significa uma dificuldade em calcular o posto algébrico.

Por outro lado, é bem mais fácil determinar pontos racionais de uma curva definida sobre um corpo finito. Por isso, uma técnica muito importante no estudo de curvas elípticas sobre $\mathbb{Q}$ é a de **redução módulo p** primo, em que, reduzindo seus coeficientes módulo p , passamos a considerá-las sobre um corpo finito. O comportamento de cada redução módulo primo é codificado numa função meromorfa chamada **L -função** da curva elíptica. A facilidade em se encontrar pontos racionais neste contexto se traduz numa facilidade em manipular esta L -função.

A **Conjectura de Birch e Swinnerton-Dyer (BSD)** foi enunciada em 1965 e permanece desafiando matemáticos ao redor do mundo. Trata-se de um dos problemas centrais da Teoria dos Números moderna, tanto que a primeira solução correta será agraciada pelo *Clay Mathematics Institute* com um prêmio de 1 milhão de dólares!^[1]

Mas não é (somente) o prêmio que desperta o grande interesse que acompanha o problema. A Conjectura BSD propõe uma solução quase milagrosa para o difícil problema de desvendar a parte que falta da estrutura das curvas elípticas sobre $\mathbb{Q}$: afirma que seu posto algébrico (algo difícil de calcular) é exatamente a ordem da L -função da curva elíptica em $s = 1$, chamada convenientemente de **posto analítico** (algo fácil de calcular)!^[2] Com isso, diversas questões que dependem de saber calcular o posto algébrico (problemas em aberto como o Problema do

^[1]Veja [Wiles \(2000\)](#) para a descrição oficial do problema.

^[2]E quando a conjectura foi formulada, nem sequer se sabia se a L -função de uma curva elíptica estaria definida em $s = 1$! Isto só veio décadas mais tarde com o trabalho de [Taylor e Wiles \(1995\)](#) e [Breuil et al. \(2001\)](#), que resultou no Teorema da Modularidade, considerada por muitos a joia da coroa da Teoria dos Números do século XX.

Número Congruente, a determinação dos pontos racionais de uma curva elíptica, entre outros) seriam esclarecidas.

Muitos avanços já foram feitos em direção à veracidade da conjectura: esta foi verificada computacionalmente em diversos casos; Gross e Zagier (1986) demonstraram que, se uma curva elíptica possui infinitos pontos racionais então sua L -função tem zero em $s = 1$, estendendo um resultado de Coates e Wiles (1977); Kolyvagin (1988), Rubin (1991), e muitos outros, mostraram a conjectura para curvas elípticas com posto analítico 0 ou 1.^[3] Por outro lado, quase nenhum avanço foi feito para curvas elípticas com posto analítico maior que 1.

Um resultado de Bhargava, Skinner e Zhang (2014) aborda o problema de uma maneira curiosa: estima por baixo a proporção das curvas elípticas que satisfazem a conjectura, calculando a densidade de um conjunto formado pelas curvas elípticas que satisfazem certas condições (algumas fáceis de se verificar, outras nem tanto) que garantem que uma curva elíptica possua posto analítico e algébrico 0 ou 1 (e, em particular, satisfaça a conjectura BSD). Desta maneira, chega-se à conclusão de que *a maioria das curvas elípticas satisfaz a Conjectura de Birch e Swinnerton-Dyer!* Mais precisamente, mostraram que a Conjectura BSD é válida para pelo menos 66,48% das curvas elípticas sobre $\mathbb{Q}$. Se for válida uma conjectura sobre o tamanho médio dos **grupos de Selmer**^[4] das curvas elípticas (Conjectura de Bhargava, 5.3.8), o método usado poderia ser extrapolado para mostrar que 100% das curvas elípticas sobre $\mathbb{Q}$ satisfazem a Conjectura BSD! Esse incrível fato é o assunto central desta dissertação.

Como organizamos o conteúdo deste trabalho

- O Capítulo 1 é uma coleção de pré-requisitos e tópicos que não tratam diretamente de curvas elípticas, mas que serão abundantemente usados para discuti-las;
- Os Capítulos 2 e 3 trazem as principais propriedades sobre curvas elípticas, partindo de corpos mais gerais, como os p -ádicos, e se afunilando até chegar em $\mathbb{Q}$, que é destacado num capítulo próprio;
- O Capítulo 4 prepara as últimas ferramentas que faltam: os grupos de Selmer e de Tate–Shafarevich;
- O Capítulo 5, o centro do texto, discute o artigo *A majority of elliptic curves over $\mathbb{Q}$ satisfies the Birch and Swinnerton-Dyer conjecture*, de Bhargava, Skinner e Zhang (2014);
- O apêndice traz mais coisas interessantes sobre a conjectura BSD que acabaram sem um lugar no texto principal.

^[3]Pode parecer pouco, mas acredita-se que estes são quase todos os casos!

^[4]Os grupos de Selmer são uma das principais fontes de informação sobre o posto algébrico que temos. Mais detalhes sobre eles no Capítulo 4.

Um guia modular

Ao estruturar o texto, priorizamos organizar os tópicos por assunto, de modo que ficasse mais fácil localizar e consultar uma definição ou resultado específico sempre que necessário. Isso faz com que uma leitura linear de todo texto seja, apesar de possível, não recomendada (e não muito eficiente). Em vez disso, organizamos as seções do texto por blocos de assunto, a fim de que o leitor possa personalizar sua rota de leitura de acordo com suas preferências:

- *Bloco Básico*: 1.1 $\rightarrow$ 2.1 $\rightarrow$ 1.4 $\rightarrow$ 2.2;
- *Bloco Modularidade*: 1.7 $\rightarrow$ 1.8;
- *Bloco BSD*: 3.1 $\rightarrow$ 3.2 $\rightarrow$ 3.3 (as subseções de todas as seções podem ser puladas; pré-requisitos recomendados: Básico, Modularidade (para a seção 3.2));
- *Bloco BSD Extra*: 3.3 $\rightarrow$ A (pré-requisitos recomendados: Básico, BSD, Modularidade (pelo menos a seção 1.7));
- *Bloco p -Ádico*: 1.4 $\rightarrow$ 1.5 $\rightarrow$ 2.3 (opcional) $\rightarrow$ 2.4 (pré-requisitos recomendados: Básico, Modularidade);
- *Bloco Galois*: 1.6 $\rightarrow$ 3.4 (pré-requisitos recomendados: Básico, p -ádico (apenas para a prova da Proposição 3.4.8 – pode ser pulada));
- *Bloco Selmer*: 1.2 $\rightarrow$ 4.1 $\rightarrow$ 4.2 $\rightarrow$ 4.3 (exceto 4.3.4; pré-requisitos recomendados: Básico);
- *Bloco Selmer Extra*: 1.3 $\rightarrow$ 4.3.4 (este bloco só é usado em algumas provas dos teoremas da Seção 5.3; pré-requisitos recomendados: Selmer);
- *Bloco Artigo*: 5.1 $\rightarrow$ 5.2 $\rightarrow$ 5.3 $\rightarrow$ 5.4 (pré-requisitos recomendados: Básico, BSD, p -Ádico e Selmer; Selmer Extra só é necessário em algumas provas da Seção 5.3);

Indicamos a seguinte ordem: Básico $\rightarrow$ Modularidade $\rightarrow$ BSD $\rightarrow$ p -Ádico $\rightarrow$ Galois $\rightarrow$ Selmer $\rightarrow$ Selmer Extra $\rightarrow$ Artigo $\rightarrow$ BSD Extra.

PRELIMINARES

Começaremos com uma exposição resumida, à guisa de vocabulário, de diversos conceitos básicos que precisaremos ao longo do texto. Os detalhes podem ser encontrados nas referências que mencionaremos no decorrer das seções.

1.1 Tópicos de curvas algébricas^[5]

1.1.1 Variedades algébricas

Seja K um corpo. O **espaço afim** de dimensão n sobre K , denotado $\mathbb{A}^n(K)$, é simplesmente o espaço vetorial K^n , cuja origem “esquecemos”. No caso $n = 2$, dizemos **plano afim**. Os automorfismos de $\mathbb{A}^n(K)$ são transformações lineares de $\text{GL}_n(K)$ compostas com translações.

Seja $I \subseteq K[x_1, \dots, x_n]$ um ideal. O **conjunto algébrico afim** associado a I é o conjunto dos zeros comuns de todos os elementos deste ideal:

$$V(I) \doteq \{P \in \mathbb{A}^n(K); f(P) = 0, \forall f \in I\}.$$
^[6]

Pelo Teorema da Base de Hilbert (BORGES; TENGAN, 2015, p. 184), I é finitamente gerado. Logo, conjuntos algébricos afins são soluções de sistemas finitos de equações polinomiais. Entre as propriedades satisfeitas pelos conjuntos algébricos afins, temos:

- $\mathbb{A}^n(K)$ e $\emptyset$ são conjuntos algébricos afins;
- $V(f) \cup V(g) = V(fg)$;
- $\bigcap_{\alpha \in A} V(I_\alpha) = V\left(\sum_{\alpha \in A} I_\alpha\right)$.

^[5]A referência básica para esta seção é Fulton (2008).

^[6]Quando necessário, explicitaremos o corpo K sobre o qual um conjunto algébrico afim V está definido escrevendo $V(K)$.

Em particular, os conjuntos algébricos afins são os fechados de uma topologia em $\mathbb{A}^n(K)$, chamada **topologia de Zariski**^[7]. Conjuntos algébricos irredutíveis com relação a esta topologia são chamados **variedades algébricas afins**. Pode-se verificar que todo conjunto algébrico afim pode ser decomposto unicamente como uma união finita de subvariedades algébricas afins.

O produto cartesiano $\mathbb{A}^m(K) \times \mathbb{A}^n(K)$ pode ser identificado com $\mathbb{A}^{m+n}(K)$. Se $V \subseteq \mathbb{A}^m(K)$ e $W \subseteq \mathbb{A}^n(K)$ são variedades afins, então $V \times W \subseteq \mathbb{A}^{m+n}(K)$ é uma variedade afim.

A **dimensão** de uma variedade algébrica V é recursivamente definida por

$$\dim(V) \doteq 1 + \max\{\dim(W); W \text{ subvariedade própria de } V\},$$

e definimos $\dim(\emptyset) \doteq -1$. A dimensão de um conjunto algébrico afim é a maior dentre as dimensões de suas componentes irredutíveis.

Uma **curva algébrica afim** é um conjunto algébrico afim de dimensão 1. Se a curva está contida no plano afim, dizemos que a curva é plana.

Inversamente, o **ideal** associado a um subconjunto (qualquer) $V \subseteq \mathbb{A}^n(K)$ é o conjunto dos polinômios que se anulam simultaneamente nos pontos de V :

$$I(V) = \{f \in K[x_1, \dots, x_n]; f(P) = 0, \forall P \in V\}.$$

Temos que V é uma variedade algébrica afim se, e somente se, $I(V)$ é primo. Em particular, podemos considerar o **anel de coordenadas** de V

$$\Gamma(V) \doteq \frac{K[x_1, \dots, x_n]}{I(V)},$$

que é um domínio, e seu corpo de frações $K(V) \doteq \text{Frac}(\Gamma(V))$, chamado **corpo de funções racionais** de V . Uma função racional pode ter **polos**, isto é, pontos em que o denominador de qualquer representação dela sempre se anula. Os demais pontos são chamados **regulares**. Tanto o conjunto dos polos quanto o conjunto dos zeros de uma função racional não-nula são subconjuntos algébricos próprios de V . Em particular, se C é uma curva irredutível, cada função racional não-nula de C admite apenas finitos zeros e polos.

Uma função racional é **regular** se não tem polos. As únicas funções para as quais todos os pontos são regulares são os próprios elementos de $\Gamma(V)$, que é por isto também denominado **anel de funções regulares** de V .

Considere a relação de equivalência em $\mathbb{A}^{n+1}(K) - \{(0, \dots, 0)\}$ dada por

$$(a_1, \dots, a_{n+1}) \sim (b_1, \dots, b_{n+1}) \iff \exists \lambda \in K^\times, a_i = \lambda b_i, \forall i \in \{1, \dots, n+1\}.$$

^[7]Uma propriedade interessante desta topologia é que abertos não-vazios são densos. Assim, como fechados são “magros”, é de se esperar que subconjuntos abertos de um fechado, sendo quase tão grandes quanto o próprio fechado que os contém, “guardem informações” do mesmo.

O **espaço projetivo** de dimensão n sobre K é definido por

$$\mathbb{P}^n(K) \doteq \mathbb{A}^{n+1}(K) - \{(0, \dots, 0)\} / \sim.$$

Denotamos a classe de equivalência de $(a_1, \dots, a_{n+1})$ por $(a_1 : \dots : a_{n+1})$. O grupo de automorfismos de $\mathbb{P}^n(K)$ é $\text{PGL}_n(K)$.

Seja U_i o conjunto dos pontos com $a_i \neq 0$ (podemos supor $a_i = 1$, sem perda de generalidade). Identificando $(a_1 : \dots : a_{i-1} : 1 : a_{i+1} : \dots : a_{n+1}) \in U_i$ com $(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_{n+1}) \in \mathbb{A}_n(K)$, podemos ver U_i como uma cópia do espaço afim dentro do espaço projetivo. Por isto, cada U_i é chamado **carta afim** de $\mathbb{P}^n(K)$. Normalmente, identificamos $\mathbb{A}^n(K)$ com a carta U_{n+1} . Os pontos restantes, que satisfazem $a_{n+1} = 0$, são os “pontos no infinito”.

Em particular, no caso do **plano projetivo** ($n = 2$), cada ponto no infinito é essencialmente a intersecção de uma, e apenas uma, família de retas paralelas de $\mathbb{A}^2(K)$. Por exemplo, $(0 : 1 : 0)$ é a intersecção das retas da forma $x = a \in K$, isto é, as retas verticais.

Podemos tentar adaptar os conceitos do mundo afim para o mundo projetivo. A primeira dificuldade que aparece é que não está bem definido avaliar um polinômio num ponto projetivo, pois o valor do polinômio no ponto pode depender do representante de classe escolhido. Porém, fica bem definido dizer se um ponto projetivo é ou não zero de um polinômio homogêneo, isto é, um polinômio $F \in K[x_1, \dots, x_{n+1}]$ tal que existe $d \in \mathbb{N}$ (o grau de F) com

$$F(\lambda x_1, \dots, \lambda x_{n+1}) = \lambda^d F(x_1, \dots, x_{n+1}), \quad \forall \lambda \in K.$$

Além disso, como todo polinômio pode ser expresso unicamente como uma soma de polinômios homogêneos de graus distintos, dizemos que um ponto projetivo é zero dele se for zero de todas as suas componentes homogêneas.

Outra particularidade notável do caso projetivo é que os ideais considerados serão homogêneos, isto é, gerados por (finitos) polinômios homogêneos.

É imediato adaptar os conceitos de conjunto algébrico, topologia de Zariski, variedade algébrica, dimensão, curva algébrica e ideal de um subconjunto de $\mathbb{P}^n(K)$. O **anel de coordenadas homogêneas** de uma variedade algébrica projetiva V é definido analogamente por

$$\Gamma_h(V) \doteq \frac{K[x_1, \dots, x_{n+1}]}{I(V)}.$$

Porém, a definição de corpo de funções racionais como antes não funciona: novamente pelo fato de pontos projetivos serem classes de equivalência de pontos afins múltiplos, simplesmente quocientar dois polinômios pode não definir função. Por isto, nem todo elemento de $K_h(V) \doteq \text{Frac}(\Gamma_h(V))$ é uma função em V . Assim, o **corpo de funções racionais** será

$$K(V) \doteq \left\{ z \in K_h(V); z = \frac{f}{g}, \text{ com } f, g \in \Gamma_h(V) \text{ de mesmo grau} \right\},$$

isto é, o subcorpo das funções que realmente fazem sentido. Definem-se polos e pontos regulares como antes^[8]. Diferentemente do caso afim, o anel de coordenadas homogêneas não é o anel das funções regulares: apenas as funções constantes é que são regulares em todos os pontos de uma variedade algébrica projetiva. Podemos, porém, trabalhar localmente: dado $P \in V$, o **anel de funções regulares em P** é definido por

$$\mathcal{O}_P(V) \doteq \{z \in K(V); z \text{ é regular em } P\}.$$

Este anel é local, e seu ideal maximal é dado pelas funções que se anulam em P .

O espaço afim, identificado como uma carta do espaço projetivo, é um aberto de Zariski de $\mathbb{P}^n(K)$. Logo, podemos considerar o fecho projetivo (o fecho na topologia de Zariski) de um conjunto algébrico de $\mathbb{A}^n(K)$, que será um fechado de $\mathbb{P}^n(K)$. Este pode ser obtido simplesmente homogeneizando os polinômios que o determinam, isto é, se $V = V(f_1, \dots, f_m)$, $\bar{V} = V(F_1, \dots, F_m)$, onde

$$F_i = x_{n+1}^{\deg(f_i)} f_i \left(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}} \right),$$

a **homogeneização** de f_i com relação à variável x_{n+1} . Inversamente, podemos considerar a intersecção de um conjunto algébrico projetivo V com uma carta U_i : este será um conjunto algébrico afim V_i que pode ser obtido desomogeneizando os polinômios que o determinam na variável x_i , isto é, se $V = V(F_1, \dots, F_m)$, então $V_i = V(f_1, \dots, f_m)$, onde

$$f_i = F_i(x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_{n+1}),$$

a **desomogeneização** de F_i com relação à variável x_i .

1.1.2 Propriedades específicas de curvas algébricas

Seja $C = V(f_1, \dots, f_m) \subseteq \mathbb{A}^n(K)$ uma curva algébrica afim^[9]. Dizemos que C possui uma **singularidade** num ponto P se a matriz $\left[\frac{\partial f_i}{\partial x_j}(P) \right]_{m \times n}$ tem posto menor que $n - 1$. Caso contrário, P é um ponto regular de C (e o posto desta matriz será exatamente $n - 1$). Se $C = V(f) \subseteq \mathbb{A}^2(K)$ é uma curva plana, $P \in C$ é singular se anula ambas as derivadas parciais de f . Uma curva que possui uma singularidade é dita **singular**.

Seja $C = V(f) \subseteq \mathbb{A}^2(K)$ uma curva plana, onde f é um polinômio de grau d . Decomponha f em componentes homogêneas como $f = f_m + \dots + f_d$. A **multiplicidade** de C em $P = (0, 0)$ ^[10] é $m_P(C) \doteq m$. Note que P é singular se, e somente se, $m > 1$: no fecho algébrico $\bar{K}$, f_m se fatora como um produto de termos lineares e cada termo linear define uma reta tangente a C em P .

^[8]Com o adicional cuidado de não anular todas as coordenadas, visto que $(0 : \dots : 0)$ não está definido!

^[9]As definições a seguir são todas locais. Portanto, para uma curva projetiva, basta reduzir ao caso afim, tomando a intersecção com uma carta afim adequada.

^[10]Para definir a multiplicidade de C em um ponto qualquer, basta tomar uma translação adequada que o coloque na origem e proceder como descrito.

Se as retas tangentes a C em um ponto singular P são todas distintas, dizemos que P é uma singularidade **ordinária**.

Sejam $C = V(f)$ e $D = V(g)$ duas curvas planas e $P \in C \cap D$. A **multiplicidade de intersecção** de C e D em P , denotada $(C, D)_P$, é um inteiro positivo que mede a ordem de contato de C e D em P . Em particular,

- $(C, D)_P \geq m_P(C)m_P(D)$, e vale a igualdade se, e somente se, C e D não têm retas tangentes em comum em P ;
- $(V(f), V(gh))_P = (V(f), V(g))_P + (V(f), V(h))_P$, para todo $h \in K[x, y]$;

Ao contar pontos na intersecção $C \cap D$, é importante levar em conta a multiplicidade:

Teorema 1.1.1 (Bézout). Sejam $C = V(F)$ e $D = V(G)$ curvas planas projetivas sobre um corpo algebricamente fechado sem componentes irredutíveis em comum. Então^[11],

$$\sum_{P \in C \cap D} (C, D)_P = \deg(F) \deg(G).$$

Uma maneira usual de representar a intersecção de duas curvas $C = V(F)$ e $D = V(G)$ é por um **(0-)ciclo de intersecção**^[12]

$$C \cdot D = \sum_{P \in \mathbb{P}^2(K)} (C, D)_P P.$$

Por fim, mencionaremos um caso particular de um teorema de Max Noether:

Teorema 1.1.2 (Max Noether). Se $V(F)$ é irredutível e $V(H) \cdot V(F) \geq V(G) \cdot V(F)$, então existe uma curva $V(L)$ tal que

$$V(L) \cdot V(F) = V(H) \cdot V(F) - V(G) \cdot V(F).$$

Em outras palavras, se a intersecção de $V(F)$ e $V(G)$ está contida, com as devidas multiplicidades, na intersecção de $V(F)$ e $V(H)$, existe uma outra curva $V(L)$ que “coleta” os pontos que sobram num outro ciclo de intersecção com $V(F)$.

1.1.3 Mapas entre variedades algébricas

Sejam $V_1 \subseteq \mathbb{A}^m(K)$ e $V_2 \subseteq \mathbb{A}^n(K)$ variedades algébricas afins. Um **morfismo** $\varphi: V_1 \rightarrow V_2$ é um mapa que é polinomial em cada coordenada, isto é, $\varphi = (f_1, \dots, f_n)$, onde $f_i \in \Gamma(V_1)$. Um **isomorfismo** é um morfismo que é invertido por outro morfismo.

^[11]O lado esquerdo da equação representa o número de pontos na intersecção das curvas, contados “corretamente”.

^[12]O 0 vem da dimensão de um ponto. Mais geralmente, em $\mathbb{P}^n$, um m -ciclo, com $m \leq n$, é uma combinação linear formal finita de variedades algébricas de dimensão m .

Similarmente, um **mapa racional** $\varphi: V_1 \dashrightarrow V_2$ é um mapa que é racional em cada coordenada, isto é, $\varphi = (z_1, \dots, z_n)$, onde $z_i \in K(V_1)$. Note que um mapa racional não está definido na variedade toda^[13], mas num aberto, que é o complementar do conjunto dos polos de cada z_i , um subconjunto algébrico de V_1 (que são os polos de φ ; nos outros pontos, dizemos que φ é **regular**). Se a imagem de φ é densa, o mapa racional é chamado **dominante**. Um **mapa birracional** é um mapa racional que é invertido por outro mapa racional^[14].

Note que um mapa racional que é regular em todo ponto de V_1 é um morfismo. Por isto, também chamamos morfismos de **mapas regulares**.

No caso projetivo, um **morfismo (mapa regular)** $\varphi: V_1 \rightarrow V_2$ também é um mapa polinomial em cada coordenada, isto é, $\varphi = (f_1 : \dots : f_{n+1})$, onde $f_i \in \Gamma_h(V_1)$, mas os polinômios devem ter mesmo grau e os pontos de V_1 não podem anular simultaneamente todos os f_i . Um **mapa racional** $\varphi: V_1 \dashrightarrow V_2$, assim como no caso afim, é um mapa localmente regular, isto é, uma classe da relação de equivalência

$$(U, \alpha) \sim (V, \beta) \iff \alpha|_{U \cap V} = \beta|_{U \cap V},$$

onde o par (U, α) é formado por um aberto $U \subseteq V_1$ e um mapa regular $\alpha: U \rightarrow V_2$. As outras definições são análogas.

Sejam V_1 e V_2 variedades algébricas projetivas. Um mapa racional dominante $\varphi: V_1 \dashrightarrow V_2$ induz um *pullback* injetor entre os corpos de funções racionais $\varphi^*: K(V_2) \rightarrow K(V_1)$. Disto, temos um funtor entre a categoria das variedades algébricas projetivas (onde as setas são mapas racionais dominantes) e a categoria dos corpos de funções racionais^[15] (onde as setas são morfismos injetores que fixam K). Este funtor é uma equivalência de categorias e, em particular,

V_1 e V_2 são birracionalmente equivalentes se, e somente se, $K(V_1)$ e $K(V_2)$ são K -isomorfos.

No caso de curvas, todo mapa racional não-constante é dominante. Toda curva (afim ou projetiva) é birracionalmente equivalente a (isto é, está bem definido um mapa birracional entre esta e) uma curva plana (o seu **modelo plano**, que, além disso, podemos tomar como possuindo apenas singularidades ordinárias) e a uma curva não-singular, não necessariamente plano (o seu **modelo não-singular**). Dois modelos não-singulares de uma mesma curva são sempre isomorfos, isto porque um mapa birracional entre duas curvas não-singulares é sempre um isomorfismo.

Duas curvas C_1 e C_2 definidas sobre um mesmo corpo K que são isomorfas sobre $\bar{K}$ são chamadas *twists* uma da outra. Note que, mesmo estando definidas sobre o mesmo corpo e sendo

^[13]Por isto denotamos com uma seta tracejada.

^[14]O mapa birracional é como um “isomorfismo fraco”.

^[15]Um **corpo de funções racionais** de grau n sobre K é um corpo L tal que $L \cap \bar{K} = K$ e L/K tem grau de transcendência n . Corpos de funções racionais de variedades algébricas são corpos de funções racionais também neste sentido.

isomorfas sobre $\bar{K}$, pode ocorrer que C_1 e C_2 não sejam isomorfas sobre K (veja Observação 2.1.15 adiante).

1.1.4 Gênero e o teorema de Riemann–Roch

Um dos principais invariantes birracionais^[16] de uma curva algébrica C é o seu **gênero**. Se C é uma curva plana irredutível de grau n que só possui singularidades ordinárias^[17], definimos seu gênero como sendo o inteiro não-negativo

$$g(C) \doteq \frac{(n-1)(n-2)}{2} - \sum_{P \in C(\bar{K})} \frac{m_P(C)(m_P(C)-1)}{2}.$$

O gênero de uma curva não só está intimamente conectado com as suas singularidades, mas também com o quão bem ou mal comportadas são suas funções racionais.

Se $f \in K(C)$, então f é, localmente, o quociente de duas funções regulares em P . Definimos $\text{ord}_P(a/b)$ como sendo $\text{ord}_P(a) - \text{ord}_P(b)$, onde $a, b \in \mathcal{O}_P(C)$ e ord_P é a valorização discreta no anel $\mathcal{O}_P(C)$ (Teorema 1.4.12 adiante).

Um **divisor** em C é uma combinação $\mathbb{Z}$ -linear finita formal de pontos $\sum_{P \in C} n_P P$. Denotamos o espaço dos divisores de C por $\text{Div}(C)$.

Definição 1.1.3. Seja $D = \sum_{P \in C} n_P P \in \text{Div}(C)$. Definimos o **espaço de Riemann–Roch** de D por

$$L(D) \doteq \{f \in K(C), \text{ord}_P(f) \geq -n_P, \forall P \in C\}.$$

Em outras palavras, $L(D)$ é o conjunto das funções que possuem polo em P de ordem não “pior” que n_P . Portanto, o divisor D controla quão “ruins” as funções podem ser em cada ponto.

Os espaços de Riemann–Roch são espaços vetoriais de dimensão finita. Denotamos a dimensão de $L(D)$ por $\ell(D)$.

Teorema 1.1.4 (Riemann–Roch, caso particular). Seja C uma curva não-singular e $D \in \text{Div}(C)$ tal que $\deg(D) > 2g - 2$. Então,

$$\ell(D) = \deg(D) - g + 1.$$

1.1.5 Curvas algébricas sobre corpos finitos

Seja $K = \mathbb{F}_q$ um corpo finito, onde $q = p^n$, com p primo. Um dos principais problemas da teoria de curvas algébricas sobre corpos finitos é contar o número de pontos $\mathbb{F}_q$ -racionais que uma curva possui. Um notável teorema de Hasse para curvas de gênero 1, estendido por Weil para o caso geral, nos dá uma cota superior para esta quantidade:

^[16]Isto é, uma propriedade compartilhada por curvas birracionalmente equivalentes.

^[17]Senão, trocamos C por um modelo nestas condições.

Teorema 1.1.5 (Hasse–Weil). Seja C uma curva projetiva não-singular de gênero g sobre $\mathbb{F}_q$. Então,

$$|\#C(\mathbb{F}_q) - (q + 1)| \leq 2g\sqrt{q}.$$

Ver, por exemplo (BRADY, 2017, p. 26, Teorema 8).

1.2 Tópicos de co-homologia de Galois

Começamos com diversos conceitos e resultados gerais de Álgebra^[18].

Definição 1.2.1. Sejam $(I, \leq)$ um conjunto direcionado^[19] e $\{A_i\}_{i \in I}$ uma família de grupos, tais que, dados $i, j \in I$, existem morfismos $\phi_{ij}: A_j \rightarrow A_i$ para todo $j \geq i$, de modo que $\phi_{ii} = id_{A_i}$ e que são compatíveis com composição, ou seja, se $k \geq j \geq i$, $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$. O **limite inverso** da família $\{A_i\}$ é o conjunto

$$\varprojlim_{i \in I} A_i = \left\{ (a_i)_{i \in I} \in \prod_{i \in I} A_i; a_i = \phi_{ij}(a_j), j \geq i \right\},$$

que é um grupo^[20], com operações coordenada-a-coordenada. Um grupo que é limite inverso de uma família de grupos finitos é dito **profinito**.

Definição 1.2.2. Seja G um grupo. Um grupo abeliano M é um G -**módulo** se G age sobre M de modo compatível com a operação de M , isto é, existe uma ação de grupos $\cdot: G \times M \rightarrow M$ tal que $g \cdot (m_1 + m_2) = g \cdot m_1 + g \cdot m_2$ para todo $g \in G$ e $m_1, m_2 \in M$.^[21]

Definição 1.2.3. Um **grupo topológico** é um grupo G que também é um espaço topológico, e tal que a operação do grupo $\cdot: G \times G \rightarrow G$ e a inversão $x \mapsto x^{-1}$ são funções contínuas^[22].

Proposição 1.2.4. Seja K um corpo perfeito^[23]. O grupo de Galois^[24] da extensão $\bar{K}/K$ é profinito. Mais especificamente,

$$\text{Gal}(\bar{K}/K) = \varprojlim_{L/K \text{ Galois finita}} \text{Gal}(L/K),$$

onde os morfismos são as restrições $\text{Gal}(L'/K) \rightarrow \text{Gal}(L/K)$ dadas por $\sigma \mapsto \sigma|_L$, com $L'/L/K$.

^[18]Para relembrar, se necessário, os conceitos mais básicos que assumimos aqui, recomendamos Lang (2002) para Álgebra geral, Milne (2018) para Teoria de Corpos e Galois, Dikranjan (2009) para Grupos Topológicos e Aurichi (2017) para Topologia.

^[19]Um conjunto I é **direcionado** se possui uma pré-ordem $\leq$ (isto é, uma relação reflexiva e transitiva) tal que todo par de elementos possui uma cota superior, isto é, dados $i, j \in I$, existe $k \in I$ tal que $i \leq k$ e $j \leq k$.

^[20]Além disso, é um subgrupo do produto direto $\prod_{i \in I} A_i$.

^[21]Equivalentemente, existe um morfismo de grupos $G \rightarrow \text{Aut}(M)$.

^[22] $G \times G$ considerado com a topologia produto.

^[23]Um corpo é **perfeito** se (dentre outras formas equivalentes) o fecho separável de K contido num fecho algébrico fixado $\bar{K}$ é o próprio $\bar{K}$.

^[24]Se L/K é uma extensão de corpos, o **grupo de Galois** da extensão é o conjunto dos automorfismos de L que fixam os elementos de K , que é um grupo com a composição.

Para cada $\sigma \in \text{Gal}(\bar{K}/K)$, seja

$$U_\sigma(L) = \sigma \cdot \ker(\text{Gal}(\bar{K}/K) \rightarrow \text{Gal}(L/K)).$$

O conjunto $\{U_\sigma(L); \sigma \in \text{Gal}(\bar{K}/K), L/K \text{ Galois finita}\}$ é a base de uma topologia em $\text{Gal}(\bar{K}/K)$, chamada **topologia de Krull**, fazendo deste grupo um grupo topológico.

Proposição 1.2.5. O grupo de Galois de uma extensão Galois qualquer L/K , com a topologia de Krull, é Hausdorff, compacto e totalmente desconexo (RIBES, 2013, p. 185, Proposição 1.6).

Agora, estamos prontos para definir os grupos de co-homologia^[25]. Sejam K um corpo perfeito e M um $\text{Gal}(\bar{K}/K)$ -módulo. Para simplificar a notação, faça $G \doteq \text{Gal}(\bar{K}/K)$.

Definição 1.2.6. O 0-ésimo grupo de co-homologia de M é o subgrupo fixo pela ação de G :

$$H^0(G, M) \doteq \{m \in M; m^\sigma = m, \forall \sigma \in G\}.$$

Um **1-cociclo** de G para M é um mapa $\xi: G \rightarrow M$ tal que

$$\xi(\sigma\tau) = \xi(\sigma) + \xi(\tau)^\sigma.$$

O conjunto dos 1-cociclos de G para M é um grupo abeliano denotado $Z^1(G, M)$. Considerando em M a topologia discreta e em G da topologia de Krull, o subgrupo dos 1-cociclos contínuos com relação a essas topologias é denotado por $Z_{\text{cont}}^1(G, M)$. O subconjunto

$$B^1(G, M) = \{\xi \in Z^1(G, M); \exists m \in M, \xi(\sigma) = m^\sigma - m, \forall \sigma \in G\}$$

é um subgrupo de $Z_{\text{cont}}^1(G, M)$, e seus elementos são chamados **1-cobordos** de G para M .

Definição 1.2.7. O primeiro grupo de co-homologia de M é definido por

$$H^1(G, M) \doteq \frac{Z_{\text{cont}}^1(G, M)}{B^1(G, M)}.$$

Observação 1.2.8. Se G age trivialmente sobre M , então

$$H^0(G, M) = M \quad \text{e} \quad H^1(G, M) = \text{Hom}_{\text{cont}}(G, M),$$

onde $\text{Hom}_{\text{cont}}(G, M)$ denota o conjunto de morfismos de grupos contínuos de G em M .

A partir de uma sequência exata de G -módulos, obtemos uma sequência exata longa envolvendo os grupos de co-homologia que definimos acima (SILVERMAN, 2009, p. 419, Proposição B.2.3):

^[25]Para o escopo deste trabalho, só precisaremos do 0-ésimo e do primeiro grupos de co-homologia. Mais informações sobre co-homologia de Galois podem ser encontradas em (SERRE, 1997). Para um pouco de intuição e motivação para as definições a seguir, redirecionamos o leitor a (MILNE, 2013, Capítulo 2.I) e, para o caso específico do primeiro grupo de co-homologia, mencionamos também a seguinte *thread* do *Mathematics Stack Exchange*: <<https://math.stackexchange.com/questions/143548/motivation-behind-the-ingredients-of-first-cohomology-group-h1>>.

Proposição 1.2.9. Considere a sequência exata de G -módulos

$$0 \longrightarrow P \longrightarrow M \xrightarrow{\psi} N \longrightarrow 0.$$

Então, existe uma sequência exata longa

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(G, P) & \longrightarrow & H^0(G, M) & \longrightarrow & H^0(G, N) \\ & & & & & & \downarrow \delta \\ & & & & H^1(G, P) & \longrightarrow & H^1(G, M) \longrightarrow H^1(G, N), \end{array}$$

onde o morfismo de conexão δ é definido da seguinte forma: se $n \in H^0(G, N) = N^G$, tome $m \in \psi^{-1}(n)$ e considere o mapa $\xi: G \rightarrow M$ dado por $\sigma \mapsto m^\sigma - m$, que é um elemento de $Z_{\text{cont}}^1(G, P)$. Definimos $\delta(n)$ como sendo a classe de ξ no quociente $H^1(G, P)$.

Seja L/K uma extensão de Galois finita. Como $\text{Gal}(\bar{K}/L)$ é um subgrupo normal de índice finito de G , podemos ver M como um $\text{Gal}(\bar{K}/L)$ -módulo. Logo, a inclusão natural induz uma restrição nos grupos de co-homologia:

$$\text{Res}: H^1(G, M) \rightarrow H^1(\text{Gal}(\bar{K}/L), M).$$

Por outro lado, o submódulo fixo $M^{\text{Gal}(\bar{K}/L)}$ é naturalmente um $G/\text{Gal}(\bar{K}/L) \cong \text{Gal}(L/K)$ -módulo. Um 1-cociclo $\xi \in Z_{\text{cont}}^1(\text{Gal}(L/K), M^{\text{Gal}(\bar{K}/L)})$ pode ser estendido a $\xi \circ \pi \in Z_{\text{cont}}^1(G, M)$, onde π denota a projeção canônica $G \twoheadrightarrow \text{Gal}(L/K)$, obtendo-se um mergulho nos grupos de co-homologia:

$$\text{Inf}: H^1(\text{Gal}(L/K), M^{\text{Gal}(\bar{K}/L)}) \rightarrow H^1(G, M).$$

Combinando estes dois mapas, obtemos uma sequência exata:

Proposição 1.2.10 (Inflação-Restrição). A seguinte sequência é exata:

$$0 \longrightarrow H^1(\text{Gal}(L/K), M^{\text{Gal}(\bar{K}/L)}) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(\text{Gal}(\bar{K}/L), M)$$

(MILNE, 2013, p. 69, Proposição 1.34).

O quociente $G/\text{Gal}(\bar{K}/L)$ induz um mapa complementar ao de restrição. Seja X um conjunto de únicos representantes das classes laterais do quociente. Definimos o mapa de co-restrição $\text{Cores}: H^1(\text{Gal}(\bar{K}/L), M) \rightarrow H^1(G, M)$ por

$$\text{Cores}(\xi)(\sigma) \doteq \sum_{\tau \in X} \tau \xi(\tau^{-1} \sigma \tau_0),$$

onde τ_0 é o representante em X da classe lateral de $\sigma^{-1} \tau$, isto é, $\tau^{-1} \sigma \tau_0 \in \text{Gal}(\bar{K}/L)$.

Proposição 1.2.11. Seja L/K uma extensão de Galois finita. Então, $\text{Cores} \circ \text{Res}$ é o mapa de multiplicação por $[L : K]$ (MILNE, 2013, p. 68, Proposição 1.30).

1.2.1 Co-homologia de Galois e isomorfismos de curvas algébricas

Seja K um corpo perfeito, C uma curva algébrica não-singular sobre K e L/K uma extensão algébrica. O conjunto dos L -automorfismos de C , isto é, os L -isomorfismos $C \rightarrow C$, é um grupo com a composição, que denotamos $\text{Aut}_L(C)$ (se $L = \overline{K}$, denotamos simplesmente $\text{Aut}(C)$). Denote também o conjunto dos *twists* de C por $\text{Twist}(C)$.

$\text{Aut}(C)$ pode não ser um grupo abeliano. Mesmo assim, podemos considerar o primeiro grupo de co-homologia de $\text{Aut}(C)$ vendo-o não como um grupo, mas como um espaço com um ponto base (que seria o cociclo trivial).

Teorema 1.2.12. Há uma bijeção entre $\text{Twist}(C)$ e $H^1(G, \text{Aut}(C))$, que associa um *twist* $\phi: C' \xrightarrow{\sim} C$ de C a $[\xi_{C'}]$, onde

$$\xi_{C'}(\sigma) = \phi^\sigma \circ \phi^{-1}$$

(SILVERMAN, 2009, p. 318, Teorema X.2.2).

A ideia é que os *twists* de C “torcem” a ação do grupo de Galois sobre $\overline{K}(C)$: dado um *twist* C' de C , o isomorfismo $\Phi: \overline{K}(C) \rightarrow \overline{K}(C')$ satisfaz

$$\Phi(f)^\sigma = \Phi(\underbrace{f^\sigma \circ \xi_{C'}(\sigma)}_{\xi_{C'}(\sigma)^*(f^\sigma)}).$$

O corpo $\overline{K}(C')$ é a versão “torcida” de $\overline{K}(C)$ por $\xi_{C'}$. Reciprocamente, partindo de $[\xi] \in H^1(G, \text{Aut}(C))$, constrói-se um corpo de funções isomorfo a $\overline{K}(C)$ (e, portanto, uma curva C' $\overline{K}$ -isomorfa a C) que satisfaz a propriedade de “torção” discutida acima.

1.3 Tópicos de grupos abelianos divisíveis

Definição 1.3.1. Seja G um grupo abeliano. Um elemento $g \in G$ é **divisível** se, para todo $n \in \mathbb{Z}_{>0}$, existe $g' \in G$ tal que $g = ng'$. Em outras palavras, g é “divisível” por inteiros positivos.

O subconjunto dos elementos divisíveis G_{div} de um grupo abeliano é um subgrupo. Dizemos que G é **divisível** se todos os seus elementos o são, isto é, $G = G_{\text{div}}$.

Lema 1.3.2 (Splitting Lemma). Considere a sequência exata de grupos abelianos

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0.$$

São equivalentes:

- Existe um morfismo $\tilde{\varphi}: B \rightarrow A$ tal que $\tilde{\varphi} \circ \varphi = \text{id}_A$;
- Existe um morfismo $\tilde{\psi}: C \rightarrow B$ tal que $\psi \circ \tilde{\psi} = \text{id}_C$;

- Existe um isomorfismo $\alpha: B \rightarrow A \oplus C$, de modo que $\alpha \circ \varphi$ é a inclusão natural $A \hookrightarrow A \oplus C$ e $\psi \circ \alpha^{-1}$ é a projeção natural $A \oplus C \rightarrow C$. Em outras palavras, temos a sequência exata

$$0 \longrightarrow A \xrightarrow{\alpha \circ \varphi} \underbrace{A \oplus C}_{\cong B} \xrightarrow{\psi \circ \alpha^{-1}} C \longrightarrow 0.$$

Se alguma dessas condições ocorre, dizemos que a sequência exata **cinde** (HATCHER, 2001, p. 147).

Proposição 1.3.3. Se A é divisível, então a sequência exata da proposição anterior sempre cinde, isto é, $B \cong A \oplus C$.

Ideias da Prova. A prova se baseia no fato de que um grupo abeliano divisível A é um $\mathbb{Z}$ -módulo injetivo, isto é, se $M' \hookrightarrow M$ é um mapa injetor de $\mathbb{Z}$ -módulos, todo morfismo $f: M' \rightarrow A$ se estende para $g: M \rightarrow A$ de modo que o diagrama comuta:

$$\begin{array}{ccc} M' & \hookrightarrow & M \\ f \downarrow & \swarrow g & \\ A & & \end{array}$$

(LANG, 2002, p. 784, Lema 4.2). Disto, tomando $M' = A$, $f = \text{id}_A$, $M = B$ e sendo φ o mapa injetor, temos que g é o $\tilde{\varphi}$ procurado. $\square$

Em particular, um grupo abeliano G é a soma direta do subgrupo dos elementos divisíveis G_{div} e o subgrupo não-divisível G/G_{div} .

Para ter algo mais “palpável”, vejamos alguns exemplos de grupos divisíveis:

- Exemplo 1.3.4** (Grupos divisíveis).
- $\mathbb{Q}$ é um grupo divisível;
 - Quocientes de grupos divisíveis são divisíveis. Em particular, $\mathbb{Q}/\mathbb{Z}$ é um grupo divisível;
 - Seja p primo. A parte p -primária $G[p^\infty]$ de um grupo divisível G (isto é, o subgrupo de G formado pelos elementos cuja ordem é uma potência de p) é divisível^[26], pois morfismos de grupos abelianos se restringem às partes p -primárias. Em particular, $(\mathbb{Q}/\mathbb{Z})[p^\infty]$ é divisível.

Essencialmente, estes são todos os exemplos de grupos divisíveis:

^[26]Isto não quer dizer que todo grupo p -primário (isto é, que é igual à sua parte p -primária) é divisível (por exemplo, $\mathbb{Z}/p\mathbb{Z}$ ou qualquer outro p -grupo finito).

Teorema 1.3.5 (da Estrutura de Grupos Divisíveis). Seja G um grupo divisível. Então

$$G \cong \left(\bigoplus_{p \text{ primo}} (\mathbb{Q}/\mathbb{Z})[p^\infty]^{(I_p)} \right) \oplus \mathbb{Q}^{(I)},$$

e as cardinalidades de I_p para cada p e I são unicamente determinadas por G . (FUCHS, 1970, p. 104, Teorema 23.1)

Corolário 1.3.6. Se G é um grupo divisível p -primário, então

$$G \cong (\mathbb{Q}/\mathbb{Z})[p^\infty]^{(I_p)},$$

e a cardinalidade de I_p é unicamente determinada por G .

Prova. Se algum dos outros tipos de componentes aparecesse na decomposição, haveria elementos cuja ordem não é uma potência de p , o que não é possível. ■

1.4 Tópicos de valorizações^[27]

Definição 1.4.1. Seja K um corpo. Uma **norma** em K é uma função $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$ tal que

- $|a| = 0 \iff a = 0$;
- $|ab| = |a||b|$;
- $|a + b| \leq |a| + |b|$ (desigualdade triangular).

Adicionalmente, dizemos que uma norma é **não-arquimediana** (ou **ultramétrica**) se vale a desigualdade triangular forte

$$|a + b| \leq \max\{|a|, |b|\}.$$

Caso contrário, dizemos que a norma é **arquimediana**.

Observação 1.4.2. Todo corpo possui a **norma trivial**, que é definida por $|a| \doteq 1$, para todo $a \neq 0$, e $|0| \doteq 0$. Note que a norma trivial é ultramétrica.

Definição 1.4.3. Duas normas $|\cdot|_1$ e $|\cdot|_2$ sobre K são **equivalentes** se existe $c > 0$ tal que, para todo $a \in K$,

$$|a|_1 = |a|_2^c.$$

Uma classe de equivalência de normas sobre K é um **lugar** (arquimediano ou não-arquimediano, dependendo dos elementos da classe) sobre K . O conjunto dos lugares (resp. arquimedianos, não-arquimedianos) de K será denotado por $\mathcal{S}_K$ (resp. $\mathcal{S}_K^{\text{arq}}$, $\mathcal{S}_K^{\text{narq}}$).

^[27]Para alguns dos resultados mencionados a seguir, aludimos à sua localização no livro de Engler e Prestel (2005), onde podem ser encontradas suas demonstrações.

Definição 1.4.4. Um grupo abeliano Γ é **totalmente ordenado** se possui uma relação de ordem total $\leq$ compatível com sua soma, isto é,

$$g_1 \leq g_2 \implies g_1 + h \leq g_2 + h.$$

Um subgrupo $\Gamma' \subseteq \Gamma$ é **convexo** se, para todo $h \in \Gamma'$, $0 \leq g \leq h \implies g \in \Gamma'$. O número de subgrupos convexos próprios de Γ é chamado **posto**^[28] de Γ .

Proposição 1.4.5 (*ibid.*, Proposição 2.1.1). Um grupo abeliano totalmente ordenado é de posto 1 (isto é, seu único subgrupo convexo próprio é 0) se, e somente se, é um subgrupo de $\mathbb{R}$.

Definição 1.4.6. Seja K um corpo. Uma **valorização** em K é uma função sobrejetora $v: K \rightarrow \Gamma \cup \{\infty\}$, onde Γ é um grupo abeliano totalmente ordenado e valem as seguintes propriedades^[29]:

- $v(a) = \infty \iff a = 0$;
- $v(ab) = v(a) + v(b)$;
- $v(a + b) \geq \min\{v(a), v(b)\}$.

O grupo Γ é chamado **grupo de valores** de v . Se Γ tem posto 0, isto é, $\Gamma = 0$, dizemos que v é **trivial**. Se Γ tem posto 1 e possui um elemento positivo minimal, dizemos que v é uma **valorização discreta**.

Definição 1.4.7. Duas valorizações v_1 e v_2 sobre K são **equivalentes** se existe $\alpha > 0$ tal que, para todo $a \in K$,

$$v_1(a) = \alpha v_2(a).$$

Em particular, toda valorização discreta é equivalente a uma valorização com grupo de valores $\mathbb{Z}$, chamada **normalizada**.

Algumas normas vêm de algumas valorizações, e vice-versa:

Proposição 1.4.8. Seja v uma valorização discreta em K . Então, $|\cdot| = c^{-v(\cdot)}$, com $c > 1$ ^[30], é uma norma ultramétrica em K . Reciprocamente, se $|\cdot|$ é uma norma ultramétrica não-trivial em K , então $v(\cdot) = -\alpha \log(|\cdot|)$, com $\alpha > 0$ ^[31] é uma valorização discreta sobre K ^[32].

De agora em diante, trataremos normas equivalentes como sendo a mesma coisa, e o mesmo para as valorizações equivalentes.

^[28]Note que este conceito é diferente do posto de Γ como grupo abeliano, e que um mesmo grupo abeliano pode ter postos distintos munindo-o de ordens distintas: por exemplo, $\mathbb{Z} \times \mathbb{Z}$ com a ordem lexicográfica tem posto 2, mas com a ordem induzida por sua identificação com o subgrupo $\mathbb{Z} + \mathbb{Z}\sqrt{2} \leq \mathbb{R}$, tem posto 1.

^[29]O símbolo ∞ é definido pelas seguintes propriedades aritméticas: $\infty \geq g$ e $\infty + g = \infty$, para todo $g \in \Gamma$.

^[30]Escolhendo diferentes valores de c , obtemos normas equivalentes.

^[31]Como antes, escolhendo diferentes valores de α , obtemos valorizações equivalentes.

^[32]Note que a norma trivial corresponde à valorização trivial e vice-versa.

Definição 1.4.9. Seja K um corpo. Um subanel de $\mathcal{O} \subseteq K$ é um **anel de valorização** se, para todo $a \in K^\times$, $a \in \mathcal{O}$ ou $a^{-1} \in \mathcal{O}$.

Proposição 1.4.10 (*ibid.*, Proposição 2.1.2). Seja (K, v) um corpo de valorização. Então,

$$\mathcal{O}_v \doteq \{a \in K; v(a) \geq 0\}$$

é um anel de valorização. Reciprocamente, se $\mathcal{O} \subseteq K$ é um anel de valorização, então existe uma valorização v em K tal que $\mathcal{O} = \mathcal{O}_v$ com grupo de valores $K^\times / \mathcal{O}^\times$.

Corolário 1.4.11. Seja $\mathcal{O} = \mathcal{O}_v$ um anel de valorização em K . Então,

$$\mathfrak{m}_v \doteq \{a \in K; v(a) > 0\}$$

é o único ideal maximal de $\mathcal{O}_v$. Em particular, anéis de valorização são locais. O corpo $k_v \doteq \mathcal{O}_v / \mathfrak{m}_v$ é chamado **corpo residual** de v .

Se a valorização é discreta, podemos dizer mais ainda sobre o anel de valorização:

Teorema 1.4.12. Seja D um domínio que não é um corpo. São equivalentes:

1. D é um anel de valorização discreta;
2. D é um domínio de ideais principais local;
3. D é noetheriano local e seu ideal maximal $\mathfrak{m}$ é principal;
4. Existe $t \in R$ irredutível tal que, para cada $z \in D$ não nulo, existem únicos $u \in D^\times$ e $n \in \mathbb{Z}_{\geq 0}$ tais que $z = ut^n$.

(BORGES; TENGAN, 2015, p. 253, Teorema 10.1.6).

O gerador do ideal maximal de D é chamado de **parâmetro local** ou **uniformizador**.

Proposição 1.4.13. Seja $\mathcal{O}_v$ um anel de valorização discreta e t um parâmetro local. Então, v é normalizada se, e somente se, $v(t) = 1$.

A menos de menção em contrário, vamos supor que as valorizações discretas consideradas são normalizadas.

1.4.1 Extensões de valorizações

Seja K_2/K_1 uma extensão algébrica de corpos. Uma valorização de K_2 pode ser restrita a uma valorização em K_1 , possivelmente trivial. Reciprocamente:

Proposição 1.4.14 (*ibid.*, Teorema. 3.1.2). Seja $\mathcal{O}_1 \subseteq K_1$ um anel de valorização. Então, existe um anel de valorização $\mathcal{O}_2 \subseteq K_2$ que estende $\mathcal{O}_1$.

Ou seja, toda valorização de K_1 pode ser estendida para uma valorização em K_2 . Considere, nos termos da proposição anterior, a valorização v_i de K_i cujo anel de valorização é $\mathcal{O}_i$ e grupo de valores é Γ_i . A extensão $\mathcal{O}_1 \subseteq \mathcal{O}_2$ induz uma extensão de corpos residuais k_2/k_1 e, pelo mapa

$$K_1^\times \hookrightarrow K_2^\times \twoheadrightarrow K_2^\times / \mathcal{O}_2^\times \cong \Gamma_2,$$

cujo núcleo é $\mathcal{O}_1^\times = \mathcal{O}_2^\times \cap K_1^\times$, obtemos que $\Gamma_1 \cong K_1^\times / \mathcal{O}_1^\times$ é um subgrupo ordenado de Γ_2 . Se K_2/K_1 é finita, $[\Gamma_1 : \Gamma_2] \leq [K_2 : K_1]$ é finito, donde Γ_1 e Γ_2 têm o mesmo posto (*ibid.*, Corolário 3.2.3). Em particular, se K_1 só possui valorizações discretas e a extensão K_2/K_1 é finita, K_2 também só possuirá valorizações discretas.

1.4.2 Completamento de corpos de valorizações

Seja K um corpo munido de uma valorização discreta (normalizada) v e $|\cdot|_v = e^{-v(\cdot)}$ a norma ultramétrica associada (Proposição 1.4.8)^[33]. Assim, K é um espaço métrico com a norma $d_v(a, b) = |a - b|_v$, e poderíamos nos perguntar se K é completo com relação a d_v , isto é, se toda sequência de Cauchy na métrica d_v é convergente.

O **completamento**^[34] do espaço métrico (K, d_v) , denotado K_v , é obtido acrescentando-se a K os limites das sequências de Cauchy que não convergem. As operações naturais

$$x + y \doteq \lim_{n \rightarrow \infty} x_n + y_n \quad \text{e} \quad x \cdot y \doteq \lim_{n \rightarrow \infty} x_n y_n$$

dão a K_v estrutura de corpo, e podemos estender a valorização v para K_v fazendo

$$v(x) \doteq -\log(|x|_v) \quad (\text{para } x \neq 0) \quad \text{e} \quad v(0) \doteq \infty.$$

Em um corpo K completo com relação a uma valorização discreta v , vale o seguinte (e não-trivial) resultado:

Teorema 1.4.15 (Lema de Hensel; *ibid.*, Corolário 1.3.2). Seja (K, v) completo e $f \in \mathcal{O}_v[T]$ um polinômio. Denote por $\bar{f} \in k_v[T]$ a redução de f módulo $\mathfrak{m}_v$. Se existe $\bar{a} \in k_v$ tal que $\bar{f}(\bar{a}) = \bar{0}$ e $\bar{f}'(\bar{a}) \neq \bar{0}$, então existe único $\alpha \in \mathcal{O}_v$ tal que $f(\alpha) = 0$ e $\bar{\alpha} = \bar{a}$ ^[35].

^[33]Aqui, e denota o número de Euler (2,71828...).

^[34]Para a construção do completamento de um espaço métrico, veja [SEARCÓID \(2007\)](#), seção 10.12, p. 187.

^[35]Isto é, raízes simples de $\bar{f}$ se levantam unicamente para raízes de f .

1.5 Tópicos de números p -ádicos^[36]

Ao longo desta seção, p é um primo fixo.

Definição 1.5.1. Seja $p \in \mathbb{Z}$ um número primo. A **valorização p -ádica** é uma valorização discreta em $\mathbb{Q}$ definida da seguinte forma: se $r = p^v \frac{a}{b} \in \mathbb{Q}^\times$ está expresso na forma irredutível, definimos $v_p(r) \doteq v$, isto é, v é a diferença entre os expoentes das maiores potências que dividem o numerador e o denominador de r . Além disso, definimos $v_p(0) \doteq \infty$ ^[37].

Definição 1.5.2. A **norma p -ádica** de $x \in \mathbb{Q}^\times$ é definida por

$$|x|_p \doteq p^{-v_p(x)},$$

e $|0|_p \doteq 0$. Como vimos anteriormente, $|\cdot|_p$ é ultramétrica.

Desta noção de norma, obtemos naturalmente uma **métrica p -ádica** $d_p: \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{R}$ dada por $d_p(x, y) = |x - y|_p$ ^[38]. O espaço métrico $(\mathbb{Q}, d_p)$ obtido não é completo^[39]. O seu completamento, denotado $\mathbb{Q}_p$, é o corpo dos **números p -ádicos**.

Definição 1.5.3. O anel dos **inteiros p -ádicos** é o subanel $\mathbb{Z}_p = \{x \in \mathbb{Q}_p, |x|_p \leq 1\} \hookrightarrow \mathbb{Q}_p$. Alternativamente, $\mathbb{Z}_p$ é o anel de valorização de v_p em $\mathbb{Q}_p$.

Da mesma forma que $\mathbb{Q}$ é denso em $\mathbb{Q}_p$, $\mathbb{Z}$ é denso em $\mathbb{Z}_p$, isto é, o limite p -ádico de uma sequência de Cauchy de inteiros é um inteiro p -ádico. Para ver isto, basta, para cada $x \in \mathbb{Z}_p$ e $n \in \mathbb{N}$, tomar $\frac{a_n}{b_n} \in \mathbb{Q}$ “suficientemente próximo” (pois $\mathbb{Q}$ é denso em $\mathbb{Q}_p$), isto é,

$$\left| x - \frac{a_n}{b_n} \right|_p \leq \frac{1}{p^n} \implies \left| \frac{a_n}{b_n} \right|_p \leq \max \left\{ |x|_p, \left| x - \frac{a_n}{b_n} \right|_p \right\} \leq 1.$$

Logo, $\frac{a_n}{b_n} \in \mathbb{Z}_p \implies p \nmid b_n$, donde é possível tomar b'_n tal que $b_n b'_n \equiv 1 \pmod{p^n}$. Fazendo $x_n = a_n b'_n \in \mathbb{Z}$, obtemos uma sequência (x_n) convergente para x . Esta sequência é “compatível módulo p^n ”, satisfazendo $x \equiv x_n \pmod{p^n}$ e $x_{n+1} \equiv x_n \pmod{p^n}$. Se restringimos a escolha tomando x_n como sendo o único inteiro $0 \leq x_n \leq p^n - 1$ nas condições acima, a sequência (x_n) nestas condições passa a ser única.

A propriedade $x_{n+1} \equiv x_n \pmod{p^n}$ evoca a (única) representação de um número inteiro não-negativo na base p e significa que todos os n primeiros p -dígitos (partindo das unidades) de x_n e x_{n+1} são iguais. Ou seja, existem únicos $0 \leq b_n < p$, $n \in \mathbb{N}$, tais que $x_n = \sum_{i=0}^n b_i p^i$. As outras propriedades da sequência (x_n) nos permitem estender de modo único esta representação

^[36]A referência básica desta seção é [GOUVÊA \(1997\)](#).

^[37]0 é “infinitamente divisível” por p .

^[38]Quanto maior for a maior potência comum que divide simultaneamente x e y , mais próximos x e y estão.

^[39]Por exemplo, $(a^{p^n})_n$, com $1 < a < p - 1$, é uma sequência de Cauchy em $\mathbb{Q}$ que não converge.

para $\mathbb{Z}_p$, escrevendo cada inteiro p -ádico como uma série de potências de p com coeficientes inteiros, ou como uma sequência de p -dígitos infinita^[40], onde seu n -ésimo p -dígito corresponde ao n -ésimo p -dígito de x_n (e de seus sucessores): $x = \sum_{i=0}^n b_i p^i$. Como cada termo é divisível por potências de p cada vez maiores, tal série converge^[41].

Considerando a família $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n \in \mathbb{N}}$ com os mapas canônicos de “mudança de módulo” $\phi_{ij}: \mathbb{Z}/p^j\mathbb{Z} \rightarrow \mathbb{Z}/p^i\mathbb{Z}$, seu limite inverso é uma maneira alternativa de enxergar o anel dos inteiros p -ádicos, isto é, $\mathbb{Z}_p = \varprojlim_{i \in \mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$: o elemento que corresponde a $x \in \mathbb{Z}_p$ é, de acordo com a notação anterior, $(b_i p^i)_{i \in \mathbb{N}}$.

1.5.1 Uma decomposição útil

Pelo Lema de Hensel (Teorema 1.4.15) aplicado a $f(x) = x^{p-1} - 1$, $\mathbb{Q}_p$ contém uma raiz $(p-1)$ -ésima primitiva da unidade^[42] que, além disso, é um inteiro p -ádico. Logo, μ_{p-1} , o grupo das raízes $(p-1)$ -ésimas da unidade, é um subgrupo de $\mathbb{Z}_p^\times$ (visto que $\alpha^{p-1} = 1 \implies |\alpha|_p = 1$).

Seja $p \neq 2$ ^[43]. A seguinte decomposição será útil para a próxima subseção:

Proposição 1.5.4. Seja $x \in \mathbb{Q}_p^\times$. Então, $x = p^n u y$, com únicos $n \in \mathbb{Z}$, $u \in \mu_{p-1}$ e $y \in 1 + p\mathbb{Z}_p$.

Prova. Seja $x \in \mathbb{Q}_p^\times$. Então

$$v_p(x p^{-v_p(x)}) = v_p(x) - v_p(x) = 0.$$

Logo, $x = p^{v_p(x)} x'$, com $v_p(x') = 0 \iff x' \in \mathbb{Z}_p^\times$. Resta decompor x' .

Temos uma sequência exata

$$0 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \xrightarrow{\pi} (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow 0,$$

onde π é a projeção módulo p . Mostraremos que esta sequência cinde, ao mostrar que $\pi|_{\mu_{p-1}}$ é um isomorfismo. Como $|\mu_{p-1}| = |(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$, resta mostrar a injetividade deste mapa. Se $u_1, u_2 \in \mu_{p-1}$ têm mesma imagem, então $u_1 u_2^{-1} \in \ker(\pi) = 1 + p\mathbb{Z}_p \implies u_1 \equiv u_2 \pmod{p}$. Como as raízes $(p-1)$ -ésimas da unidade são todas distintas módulo p (Lema de Hensel, Teorema 1.4.15), $u_1 = u_2$. Logo, pelo Lema 1.3.2, a sequência exata cinde e $\mathbb{Z}_p^\times \cong \mu_{p-1} \oplus (1 + p\mathbb{Z}_p)$. ■

^[40]Esta representação em base p será finita se, e somente se, o inteiro p -ádico for, na verdade, inteiro não-negativo.

^[41]Na Análise p -ádica, uma série converge se, e somente se, seu termo geral converge para 0 (o sonho de todo estudante de Análise real!). Veja (GOUVÊA, 1997, p. 89, Corolário 4.1.2) para uma demonstração.

^[42]Na verdade, pelo lema de Hensel, $\mathbb{Q}_p$ contém uma raiz m -ésima primitiva da unidade se, e somente se, $m|p-1$.

^[43]O caso $p = 2$ também pode ser feito com alguns ajustes mas, como não vamos precisar, apenas remetemos o leitor a GOUVÊA (1997, p. 120).

1.5.2 Logaritmo p -ádico

O logaritmo complexo possui a seguinte expansão perto do 0:

$$\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}.$$

Inspirados no caso complexo, definimos:

Definição 1.5.5. Considere a bola aberta $U = \{x \in \mathbb{Z}_p; |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$. Definimos o **logaritmo p -ádico** por

$$\log_p(x) \doteq \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n} \in p\mathbb{Z}_p. \text{ [44]}$$

Esta função realmente funciona como um logaritmo, isto é,

Proposição 1.5.6. Para todo $a, b \in 1 + p\mathbb{Z}_p$, $\log_p(ab) = \log_p(a) + \log_p(b)$ (GOUVÊA, 1997, p. 113, Proposição 4.5.3).

Vamos estender o logaritmo p -ádico para $\mathbb{Q}_p^\times$, supondo $p \neq 2$. Se $x \in \mathbb{Q}_p^\times$, então, pela Proposição 1.5.4, $x = p^n uy$, com $n \in \mathbb{Z}$, $u \in \mu_{p-1}$ e $y \in 1 + p\mathbb{Z}_p$. Assim, basta definirmos $\log_p$ em p e u e colocar

$$\log_p(x) \doteq n \log_p(p) + \log_p(u) + \log_p(y).$$

Para que $\log_p$ continue satisfazendo a propriedade da Proposição 1.5.6, devemos ter que

$$(p-1) \log_p(u) = \log_p(u^{p-1}) = \log_p(1) = 0 \implies \log_p(u) = 0,$$

e definimos $\log_p(p) \doteq 0$. Com isto, $\log_p: \mathbb{Q}_p^\times \rightarrow p\mathbb{Z}_p$ está bem definido.

^[44]Se $x \in 1 + p\mathbb{Z}_p$, $v_p(x-1) \geq 1$. Observe que, para todo $n > 1$, $n \geq 2v_p(n)$ (basta reduzir ao caso em que n é potência de p). Logo,

$$v_p \left((-1)^{n+1} \frac{(x-1)^n}{n} \right) = v_p(x-1) - v_p(n) \geq \frac{n}{2} v_p(x-1).$$

Logo, os termos da série são cada vez mais divisíveis por p , isto é, $\lim_{n \rightarrow \infty} \left| (-1)^{n+1} \frac{(x-1)^n}{n} \right|_p = 0$. Como comentamos na nota [41], isto implica a convergência da série. Finalmente, para ver que $\log_p(x) \in p\mathbb{Z}_p$,

$$|\log_p(x)|_p \leq \lim_{N \rightarrow \infty} \sup_{1 \leq n \leq N} \left| (-1)^{n+1} \frac{(x-1)^n}{n} \right|_p \leq \lim_{N \rightarrow \infty} \sup_{1 \leq n \leq N} |x-1|_p = |x-1|_p < 1.$$

1.5.3 Estendendo a norma p -ádica

Seja $\mathbb{L}/\mathbb{Q}_p$ uma extensão finita e de grau n . A função $|\cdot|_p: \mathbb{L} \rightarrow \mathbb{R}_{\geq 0}$ definida por

$$|x| = \sqrt[n]{|N_{\mathbb{L}/\mathbb{Q}_p}(x)|_p},$$

onde $N_{\mathbb{L}/\mathbb{Q}_p}(x) \doteq \prod_{\sigma \in \text{Gal}(\mathbb{L}/\mathbb{Q}_p)} \sigma(x) \in \mathbb{Q}_p$ é a norma da extensão $\mathbb{L}/\mathbb{Q}_p$, é uma norma não-arquimediana em $\mathbb{L}$ que estende a norma p -ádica $\mathbb{Q}_p$ (GOUVÊA, 1997, p. 151, Teorema 5.3.5). Além disso, qualquer norma em $\mathbb{L}$ que estende $|\cdot|_p$ é equivalente (*ibid.*, p. 145, Corolário 5.3.2). Logo, podemos falar na extensão da norma p -ádica para $\mathbb{L}$, que também denotamos por $|\cdot|_p$.

Em particular, como $\overline{\mathbb{Q}_p} = \bigcup_{\mathbb{L}/\mathbb{Q}_p \text{ finita}} \mathbb{L}$, a norma p -ádica tem uma única extensão para o fecho algébrico de $\mathbb{Q}_p$, que também denotamos $|\cdot|_p$.^[45]

1.6 Tópicos de Teoria Algébrica dos Números^[46]

Seja $\mathbb{K} \subseteq \overline{\mathbb{Q}}$ um corpo de números, isto é, uma extensão finita de $\mathbb{Q}$, e denote por $\mathcal{O}$ seu anel de inteiros^[47]. Como $\mathcal{O}$ é um domínio de Dedekind^[48] (NEUKIRCH, 2009, p. 17), todo ideal primo não-nulo é maximal. Além disso, ideais funcionam como números^[49]: todo ideal não-trivial $\mathfrak{a}$ de $\mathcal{O}$ se fatora de maneira única em ideais maximais

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}. \quad (1.1)$$

Definindo, para cada $\mathfrak{p}$ maximal, o ideal fracionário^[50]

$$\mathfrak{p}^{-1} \doteq \{x \in K; x\mathfrak{p} \subseteq \mathcal{O}\}, \quad [51]$$

podemos estender a fatoração acima para os ideais fracionários de $\mathcal{O}$ (NEUKIRCH, 2009, p. 22, Corolário 3.9). Assim, o conjunto dos ideais fracionários de $\mathcal{O}$ é um grupo abeliano.

Em particular, para cada $x \in \mathbb{K}^\times$, podemos considerar o ideal fracionário $(x) \doteq x \cdot \mathcal{O}$.

^[45]No entanto, $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ não é completo (GOUVÊA, 1997, p. 181, Teorema 5.7.4). Seu completamento é o corpo $\mathbb{C}_p$, dos chamados **números complexos p -ádicos**, que além de completo é algebricamente fechado.

^[46]A referência básica desta seção é Neukirch (2009)

^[47]O **anel de inteiros** de uma extensão de $\mathbb{Q}$ é o subanel formado por todos os elementos que satisfazem equações polinomiais mônicas com coeficientes em $\mathbb{Z}$. Quando necessário, especificamos o corpo com um subscrito.

^[48]Um **domínio de Dedekind** é um domínio D noetheriano, integralmente fechado (isto é, seu fecho integral em $\text{Frac}(D)$ é ele próprio) e tal que todo ideal primo não-nulo é maximal.

^[49]Os anéis $\mathcal{O}$ podem não ser domínios de fatoração única (por exemplo, em $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$, 21 se fatora em primos como $3 \cdot 7$ e $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$). Os ideais principais seriam, portanto, os “números ideais”, para os quais haveria a fatoração única. De fato, um domínio de Dedekind é um domínio de fatoração única se, e somente se, é um domínio de ideais principais (MILNE, 2017, p. 52, Proposição 3.18).

^[50]Um **ideal fracionário** de $\mathcal{O}_K$ é um $\mathfrak{f} \subseteq K$ tal que existem $d \in \mathcal{O}_K$ e $\mathfrak{a} \subseteq \mathcal{O}_K$ um ideal tal que $\mathfrak{f} = \frac{1}{d}\mathfrak{a}$.

^[51]Para ver que $\mathfrak{p}^{-1}$ é de fato um ideal fracionário, basta escrever $\mathfrak{p} = \left(\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}\right)$ (pois $\mathcal{O}$ é noetheriano) e notar que $\mathfrak{p}^{-1} = \frac{1}{b_1 \cdots b_n} (a_1 b_2 \cdots b_n, \dots, a_i b_1 \cdots b_{i-1} b_{i+1} \cdots b_n, \dots, a_n b_1 \cdots b_{n-1})$.

Definição 1.6.1. Seja $\mathbb{K}$ um corpo de números, $x \in \mathbb{K}^\times$ e considere a fatoração de (x) como em (1.1). Fixado $\mathfrak{p} \in \text{Specm}(\mathcal{O})$, definimos a **valorização $\mathfrak{p}$ -ádica** de x como o expoente $v_{\mathfrak{p}}(x)$ de $\mathfrak{p}$ na fatoração acima. Equivalentemente, $v_{\mathfrak{p}}(x)$ é o maior inteiro d tal que $x \in \mathfrak{p}^d \mathcal{O}$.

Veremos adiante que estas são as únicas valorizações não-triviais de $\mathbb{K}$.

1.6.1 Extensões de ideais primos

Seja $\mathbb{L}/\mathbb{K}$ uma extensão finita de corpos de números e tome $\mathfrak{p} \in \text{Specm}(\mathcal{O}_{\mathbb{K}})$. Estendendo $\mathfrak{p}$ para $\mathcal{O}_{\mathbb{L}}$, obtemos um ideal $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ (que denotaremos simplesmente por $\mathfrak{p}$, quando o contexto for claro) que se fatora como

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

com $\mathfrak{P}_i \in \text{Specm}(\mathcal{O}_{\mathbb{L}})$. O número g de termos na fatoração é o **índice de decomposição** de $\mathfrak{p}$.

O **índice de ramificação** de $\mathfrak{P}_i$ com relação a $\mathfrak{p}$ é $e(\mathfrak{P}_i/\mathfrak{p}) \doteq e_i$. Se algum destes índices é maior que 1, dizemos que $\mathfrak{p}$ **ramifica** em $\mathbb{L}$. Se $e(\mathfrak{P}/\mathfrak{p}) > 0$, então $\mathfrak{P}$ aparece na fatoração de $\mathfrak{p}$, e dizemos que $\mathfrak{P}$ **divide** $\mathfrak{p}$.

Teorema 1.6.2. Apenas finitos $\mathfrak{p} \in \text{Specm}(\mathcal{O}_{\mathbb{K}})$ ramificam em $\mathbb{L}$ (NEUKIRCH, 2009, p. 49, Proposição 8.5).

Para cada i , o corpo $\mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i$ é uma extensão de $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$. Definimos o **grau residual** f_i de $\mathfrak{P}_i$ com relação a $\mathfrak{p}$ como sendo o grau desta extensão.

Teorema 1.6.3 (Igualdade Fundamental). Com a notação acima, $\sum_{i=1}^g e_i f_i = [\mathbb{L} : \mathbb{K}]$ (NEUKIRCH, 2009, p. 46, Proposição 8.2).

Até o final da subseção, suponha que a extensão $\mathbb{L}/\mathbb{K}$ é Galois. Então, seguindo a notação acima, $e_1 = \cdots = e_g \doteq e$ e $f_1 = \cdots = f_g \doteq f$ (STEIN, 2010, p. 99, Teorema 9.2.2). Neste caso, a igualdade fundamental se torna

$$[\mathbb{L} : \mathbb{K}] = efg.$$

Seja $\mathfrak{P} \in \text{Specm}(\mathbb{L})$. O **grupo de decomposição** de $\mathfrak{P}$ é o subgrupo do grupo de Galois da extensão que deixa $\mathfrak{P}$ invariante:

$$D_{\mathfrak{P}} \doteq \{\sigma \in \text{Gal}(\mathbb{L}/\mathbb{K}); \mathfrak{P}^\sigma = \mathfrak{P}\}.$$

Logo, $D_{\mathfrak{P}}$ age sobre o corpo residual $\mathcal{O}_{\mathbb{L}}/\mathfrak{P}$, e o núcleo desta ação é o **grupo de inércia** de $\mathfrak{P}$:

$$I_{\mathfrak{P}} \doteq \{\sigma \in D_{\mathfrak{P}}; x^\sigma \equiv x \pmod{\mathfrak{P}}, \forall x \in \mathcal{O}_{\mathbb{L}}\}.$$

Se $\mathfrak{P}$ divide $\mathfrak{p}$, seguindo a notação anterior, $D_{\mathfrak{P}}$ tem ordem ef (e , portanto, índice g como subgrupo do grupo de Galois), enquanto que $I_{\mathfrak{P}}$ tem índice f como subgrupo de $D_{\mathfrak{P}}$ e, portanto, ordem e . Logo, $\mathfrak{p}$ não ramificar em $\mathbb{L}$ é equivalente a $I_{\mathfrak{P}}$ ser trivial para qualquer $\mathfrak{P}$ que divide $\mathfrak{p}$.

Podemos adaptar os conceitos acima para $\overline{\mathbb{Q}}$. Seja $\overline{\mathbb{Z}}$ o fecho inteiro de $\mathbb{Z}$ em $\overline{\mathbb{Q}}$. Como

$$\overline{\mathbb{Q}} = \bigcup_{\mathbb{K}/\mathbb{Q} \text{ finita}} \mathbb{K} \quad \text{e} \quad \overline{\mathbb{Z}} = \bigcup_{\mathbb{K}/\mathbb{Q} \text{ finita}} \mathcal{O}_{\mathbb{K}},$$

um ideal maximal $\mathfrak{p} \in \text{Specm}(\overline{\mathbb{Z}})$ é da forma $\mathfrak{p} = \bigcup_{\mathbb{K}/\mathbb{Q} \text{ finita}} \mathfrak{p}_{\mathbb{K}}$, com $\mathfrak{p}_{\mathbb{K}} \in \text{Specm}(\mathcal{O}_{\mathbb{K}})$.

Como o fecho normal de uma extensão finita também é uma extensão finita, todo corpo de números $\mathbb{K}$ está contido em um corpo de números $\mathbb{F}$ Galois sobre $\mathbb{K}$. Logo, podemos trocar, nas expressões acima, $\mathbb{K}$ por $\mathbb{F}$. Pela Proposição 1.2.4, temos que

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{\mathbb{F}/\mathbb{Q} \text{ Galois finita}} \text{Gal}(\mathbb{F}/\mathbb{Q}).$$

Seja $\mathfrak{p} \in \text{Specm}(\overline{\mathbb{Z}})$. Como antes, definimos o **grupo de decomposição** de $\mathfrak{p}$ como o subgrupo do grupo de Galois da extensão que deixa $\mathfrak{p}$ invariante:

$$D_{\mathfrak{p}} \doteq \{\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}); \mathfrak{p}^{\sigma} = \mathfrak{p}\}.$$

Logo, $D_{\mathfrak{p}}$ age sobre o corpo residual $\overline{\mathbb{Z}}/\mathfrak{p} \cong \overline{\mathbb{F}}_p$, e o núcleo desta ação é o **grupo de inércia** de $\mathfrak{p}$:

$$I_{\mathfrak{p}} \doteq \{\sigma \in D_{\mathfrak{p}}; x^{\sigma} \equiv x \pmod{\mathfrak{p}}, \forall x \in \overline{\mathbb{Z}}\}.$$

1.6.2 Elementos de Frobenius

Sejam $\mathbb{F}/\mathbb{Q}$ uma extensão finita Galois, p primo e $\mathfrak{p} \in \text{Specm}(\mathbb{F})$ sobre p . A ação de $D_{\mathfrak{p}}$ sobre $\mathcal{O}_{\mathbb{F}}/\mathfrak{p} \cong \mathbb{F}_{p^f}$ pode ser vista como um mapa sobrejetor $D_{\mathfrak{p}} \twoheadrightarrow \text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ cujo núcleo é $I_{\mathfrak{p}}$. Um importante elemento de $\text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ é o **mapa de Frobenius** $\sigma_p: x \mapsto x^p$, que gera este grupo. Um elemento de $D_{\mathfrak{p}}$ na pré-imagem do mapa de Frobenius é chamado **elemento de Frobenius**, denotado $\text{Frob}_{\mathfrak{p}}$. Note que este símbolo representa, potencialmente, mais de um elemento: de fato, $\text{Frob}_{\mathfrak{p}}$ é unicamente determinado se, e somente se, $I_{\mathfrak{p}}$ é trivial, o que ocorre se, e somente se, p é não-ramificado (o que, pelo Teorema 1.6.2, ocorre para todos exceto finitos primos).

Como $\text{Gal}(\mathbb{F}/\mathbb{Q})$ age transitivamente sobre os ideais primos de $\mathcal{O}_{\mathbb{F}}$, todos os outros ideais maximais de $\mathcal{O}_{\mathbb{F}}$ são conjugados a $\mathfrak{p}$, e seus elementos de Frobenius se relacionam da seguinte forma:

$$\text{Frob}_{\mathfrak{p}^{\sigma}} = \sigma^{-1} \text{Frob}_{\mathfrak{p}} \sigma \quad \sigma \in \text{Gal}(\mathbb{F}/\mathbb{Q}).$$

Os elementos de Frobenius são importantes porque estão por toda parte:

Teorema 1.6.4 (da Densidade de Chebotarov). Para cada $\sigma \in \text{Gal}(\mathbb{F}/\mathbb{Q})$, existem infinitos $\mathfrak{p} \in \mathcal{O}_{\mathbb{F}}$ tais que $\sigma = \text{Frob}_{\mathfrak{p}}$ (WIESE, 2012, p. 11).

As considerações acima podem ser imediatamente adaptadas trocando-se $\mathbb{F}$ por $\overline{\mathbb{Q}}$: Seja $\mathfrak{p} \in \text{Specm}(\overline{\mathbb{Z}})$. Um elemento de $D_{\mathfrak{p}}$ correspondente ao mapa de Frobenius $\sigma_p \in \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ na ação de $D_{\mathfrak{p}}$ é chamado **elemento de Frobenius (absoluto)**^[52], e denotado por $\text{Frob}_{\mathfrak{p}}$. Novamente, os elementos de Frobenius estão definidos a menos de $I_{\mathfrak{p}}$.

Como antes, elemento de Frobenius de ideal conjugado é conjugado de elemento de Frobenius. Note também que, se $\mathbb{F}/\mathbb{Q}$ é uma extensão finita Galois,

$$\text{Frob}_{\mathfrak{p}}|_{\mathbb{F}} = \text{Frob}_{\mathfrak{p} \cap \mathbb{F}}.$$

Os elementos de Frobenius absolutos também estão por toda parte: de certa forma, os elementos de Frobenius são *quase* todos os elementos de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

Teorema 1.6.5. Existem infinitos $\mathfrak{p} \in \text{Specm}(\overline{\mathbb{Z}})$ para os quais, escolhendo-se um elemento de Frobenius $\text{Frob}_{\mathfrak{p}}$, o conjunto formado por estes elementos escolhidos é denso em $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Prova. Seja $U_{\sigma}(\mathbb{F})$ um aberto da base da Topologia de Krull de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Como $\sigma|_{\mathbb{F}} \in \text{Gal}(\mathbb{F}/\mathbb{Q})$, pelo Teorema da densidade de Chebotarov, $\sigma|_{\mathbb{F}}$ é um elemento de Frobenius para infinitos $\mathfrak{p} \in \text{Specm}(\mathcal{O}_{\mathbb{F}})$. Tome um, levante-o para um ideal $\mathfrak{P}$ e escolha um elemento de Frobenius $\text{Frob}_{\mathfrak{P}}$ que levanta σ . Então $\text{Frob}_{\mathfrak{P}} \sigma^{-1}|_{\mathbb{F}} = \text{id}_{\mathbb{F}} \implies \text{Frob}_{\mathfrak{P}} \in U_{\sigma}(\mathbb{F})$. ■

1.6.3 Lugares em corpos de números

Começamos com a classificação dos lugares em $\mathbb{Q}$:

Teorema 1.6.6 (Ostrowski). Os lugares não-triviais de $\mathbb{Q}$ são as classes da norma usual (o único lugar arquimediano) e as classes das normas p -ádicas, para todo p primo (GOUVÊA, 1997, p. 46, Teorema 3.1.3).

Logo, as únicas valorizações discretas não-triviais de $\mathbb{Q}$ são as valorizações p -ádicas. De fato, estas são todas as valorizações de $\mathbb{Q}$, pois os anéis de valorização contidos em $\mathbb{Q}$ são as localizações $\mathbb{Z}_{(p)}$, com p primo. Em particular, há uma bijeção entre ideais primos de $\mathbb{Z}$ e valorizações de $\mathbb{Q}$ (o ideal (0) corresponde à valorização trivial).

Seja $\mathbb{K}$ um corpo de números. Como $\mathbb{K}/\mathbb{Q}$ é finita, sabemos, da subseção 1.4.1, que todas as valorizações de $\mathbb{K}$ são discretas ou a trivial e que, portanto, estão em bijeção com os lugares não-arquimedianos de $\mathbb{K}$. A valorização trivial, como antes, corresponde ao ideal primo (0) . A uma valorização discreta v não-trivial, por sua vez, podemos associar o ideal primo $\mathfrak{m}_v$. Reciprocamente, dado um ideal primo não nulo (e, portanto, maximal) $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$, associamos a

^[52]O adjetivo “absoluto” se refere ao fecho separável/algébrico. Note que σ_p não é um gerador de $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_{n \in \mathbb{N}} \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F})$, já que este grupo é isomorfo a $\widehat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$, o grupo dos inteiros profinitos, que não é cíclico (NEUKIRCH, 2009, p. 272).

valorização p -ádica, ficando estabelecida uma bijeção entre os lugares não-arquimedianos sobre $\mathbb{K}$, as valorizações sobre $\mathbb{K}$ e os ideais primos de $\mathcal{O}_{\mathbb{K}}$ [53].

Em particular, as possíveis extensões de uma valorização discreta v_p de $\mathbb{Q}$ para um corpo numérico dependem dos primos que dividem o ideal primo (p) de $\mathbb{Z}$ a ela correspondente.

Agora, tratemos dos lugares arquimedianos dos corpos de números. Pelo Teorema de Ostrowski (Teorema 1.6.6), o único lugar arquimediano de $\mathbb{Q}$ é o da norma usual, que denotamos $|\cdot|_{\infty}$ [54]. Seja $|\cdot|$ uma norma arquimediana em $\mathbb{K}$ e denote por $\widehat{\mathbb{K}}$ o completamento de $\mathbb{K}$ com relação à métrica induzida por sua norma. Como $\mathbb{K}/\mathbb{Q}$ é finita, $\widehat{\mathbb{K}}/\widehat{\mathbb{Q}}$ é finita. Mas $\widehat{\mathbb{Q}} = \mathbb{Q}_{\infty} = \mathbb{R}$, donde $\widehat{\mathbb{K}}$ é $\mathbb{R}$ ou $\mathbb{C}$, que são as únicas extensões finitas de $\mathbb{R}$ (Teorema Fundamental da Álgebra). Nestes corpos, toda norma arquimediana é equivalente à norma usual $|\cdot|_{\infty}$ [55]. Logo, cada mergulho $\iota: \mathbb{K} \rightarrow \widehat{\mathbb{K}}$ origina uma norma arquimediana em $\mathbb{K}$, da forma $|x| = |\iota(x)|_{\infty}$ [56].

Apesar de lugares arquimedianos não surgirem de valorizações, usaremos, por simplicidade, v para nos referirmos a qualquer lugar de $\mathbb{K}$, arquimediano ou não. E assim como fizemos para valorizações (e, portanto, para lugares não-arquimedianos, que são a mesma coisa!), denotaremos o completamento de $\mathbb{K}$ com relação ao lugar v como $\mathbb{K}_v$.

1.7 Tópicos de formas modulares

O grupo multiplicativo

$$\mathrm{SL}_2(\mathbb{Z}) \doteq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}); ad - bc = 1 \right\}$$

age sobre o semiplano superior do plano complexo $\mathbb{H} \doteq \{z \in \mathbb{C}; \mathrm{Im}(z) > 0\}$ por meio de transformações de Möbius:

$$\mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} \rightarrow \mathbb{H}: \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z \right) \mapsto \frac{az + b}{cz + d}.$$

[53]Frequentemente, abusaremos da nomenclatura tomando um pelo outro.

[54]Pensar que a norma usual está associada a um “primo no infinito” fecha alguns “buracos” (além de abreviar a notação!): Por exemplo, há uma forte analogia entre $\mathbb{Q}$ e o corpo de funções algébricas $k(T)$ (ver nota [164]). Permitindo $p = \infty$ a analogia entre o Teorema dos Resíduos em $k(T)$ e sua contraparte numérica, a Fórmula do Produto (para todo $x \in \mathbb{Q}$,

$$\prod_{p \leq \infty} |x|_p = 1,$$

para todo $x \in \mathbb{Q}$ (GOUVÊA, 1997, p. 48, Proposição 3.1.4)), passa a ser bem mais evidente. Inspirando-se nisto, bem como numa tentativa de estender a analogia entre primos e lugares não-arquimedianos, fala-se também em “primos no infinito” associados a normas arquimedianas sobre um corpo qualquer.

[55]Como $\mathbb{Q}$ é denso em $\mathbb{R}$ e a norma usual (e, portanto, qualquer norma equivalente a ela) é contínua, segue do Teorema de Ostrowski a afirmação para $\mathbb{R}$. Para $\mathbb{C}$, notamos que raízes n -ésimas da unidade sempre têm norma 1, pela multiplicatividade da norma. Assim, trocamos $\mathbb{Q}$ por $\mathbb{R}e^{2\pi i\mathbb{Q}} = \{re^{2\pi iq}; r \in \mathbb{R}, q \in \mathbb{Q}\}$, que é denso em $\mathbb{C}$.

[56]Se $\widehat{\mathbb{K}} = \mathbb{R}$, cada mergulho determina um lugar distinto. Se $\widehat{\mathbb{K}} = \mathbb{C}$, os mergulhos vêm aos pares, um sendo o conjugado do outro, e cada par determina um lugar distinto (BOREVICH; SHAFAREVICH, 1966, p. 277, Seção 4.1).

A ação acima pode ser estendida para o infinito^[57] tomando limites:

$$\lim_{\text{Im}(z) \rightarrow \infty} \frac{az+b}{cz+d} = \frac{a}{c}.$$

Assim, a órbita de ∞ nesta ação é $\mathbb{Q} \cup \{\infty\}$.

Definição 1.7.1. Seja $N > 0$ inteiro. Definimos o **subgrupo de congruência principal de nível N** de $\text{SL}_2(\mathbb{Z})$ como sendo o subgrupo das matrizes que são “identidades módulo N ”:

$$\Gamma(N) \doteq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}), \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$$

(onde a congruência módulo N de matrizes significa que cada entrada da primeira matriz é congruente módulo N à sua respectiva entrada na outra matriz).

Um subgrupo $\Gamma \leq \text{SL}_2(\mathbb{Z})$ é um **subgrupo de congruência** de $\text{SL}_2(\mathbb{Z})$ se contém $\Gamma(N)$, para algum N . O menor de todos os N nestas condições é chamado **nível** de Γ .

Note que $\Gamma(N)$ é o núcleo da projeção canônica $\text{SL}_2(\mathbb{Z}) \twoheadrightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Logo, todo subgrupo de congruência do $\text{SL}_2(\mathbb{Z})$ tem índice finito.

Observe que a ação de $\text{SL}_2(\mathbb{Z})$ sobre $\mathbb{H}$ por transformações de Möbius pode ser restrita a um subgrupo de congruência Γ . Se tentamos estender a ação de Γ para ∞ como antes, pode ocorrer que, para certo $r \in \mathbb{Q}$, as matrizes que transportam ∞ a r estão ausentes, dividindo a $\text{SL}_2(\mathbb{Z})$ -órbita de ∞ em várias (porém finitas, pela finitude de $[\text{SL}_2(\mathbb{Z}) : \Gamma]$) órbitas, particionando $\mathbb{Q} \cup \{\infty\}$. A estas órbitas chamamos **cúspides** de Γ .

Exemplo 1.7.2. Os seguintes exemplos de subgrupos de congruência serão importantes:

$$\begin{aligned} \Gamma_0(N) &\doteq \left\{ \gamma \in \text{SL}_2(\mathbb{Z}), \gamma \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\}, \\ \Gamma_1(N) &\doteq \left\{ \gamma \in \text{SL}_2(\mathbb{Z}), \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}. \end{aligned}$$

onde $*$ indica ausência de restrição. Temos que

$$\Gamma(N) \trianglelefteq \Gamma_1(N) \trianglelefteq \Gamma_0(N) \leq \text{SL}_2(\mathbb{Z})$$

($\Gamma_0(N)$ nem sempre é normal em $\text{SL}_2(\mathbb{Z})$). Note também que

$$\text{SL}_2(\mathbb{Z}) = \Gamma(1) = \Gamma_0(1) = \Gamma_1(1).$$

^[57]A compactificação de Alexandroff de $\mathbb{C}$. Usualmente pensamos nele como o “topo” do eixo imaginário.

Antes de definirmos o objeto principal desta seção, precisamos de um conceito preliminar, que também será utilizado adiante.

Definição 1.7.3. Seja $f: \mathbb{H} \rightarrow \mathbb{C}$, $k \in \mathbb{Z}_{\geq 0}$ e $\alpha \in \mathrm{GL}_2^+(\mathbb{Q}) \doteq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{Q}); ad - bc > 0 \right\}$. Definimos o **operador α -colchete de peso k** que age sobre f por

$$f[\alpha]_k(z) \doteq (\det \alpha)^{k-1} j(\alpha, z)^{-k} f(\alpha \cdot z),$$

onde $j(\alpha, z) \doteq cz + d$ é o **fator de automorfia** de $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Note que, se $\alpha_1, \alpha_2 \in \mathrm{GL}_2^+(\mathbb{Q})$, $j(\alpha_1 \alpha_2, z) = j(\alpha_1, \alpha_2 \cdot z) j(\alpha_2, z)$. Em particular, o colchete é “multiplicativo”: $f[\alpha_1 \alpha_2]_k = (f[\alpha_1]_k)[\alpha_2]_k$.

Definição 1.7.4. Seja $k \in \mathbb{Z}_{\geq 0}$ e $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ de congruência de nível N . Uma função $f: \mathbb{H} \rightarrow \mathbb{C}$ é uma **forma Γ -modular de peso k** se satisfizer:

- (i) f é holomorfa em $\mathbb{H}$;
- (ii) $f[\gamma]_k(z) = f(z)$, para todo $\gamma \in \Gamma$. Em particular, f é periódica, pois $\begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} \in \Gamma$;
- (iii) Seja h o menor natural tal que $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \Gamma$. Para todo $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $f[\alpha]_k$ se expande “em torno da cúspide $\alpha \cdot \infty$ ” como^[58]

$$f[\alpha]_k(z) = \sum_{n=0}^{\infty} a_n(f[\alpha]_k) q_h^n \quad (q_h = e^{2\pi i z/h}).$$

A condição (iii) é chamada de holomorficidade nas cúspides de Γ .

Se f se anula em todas as cúspides (isto é, $a_0(f[\alpha]_k) = 0$ para todo $\alpha \in \mathrm{SL}_2(\mathbb{Z})$), dizemos que f é uma **forma Γ -cúspide de peso k** .

Exemplo 1.7.5 (Série de Eisenstein). Seja $k \geq 4$ inteiro. Definimos a **série de Eisenstein** de peso k por

$$G_k(z) \doteq \sum_{(m,n) \in \mathbb{Z}^2 - \{(0,0)\}} \frac{1}{(mz + n)^k},$$

que é um exemplo de forma $\mathrm{SL}_2(\mathbb{Z})$ -modular de peso k (SERRE, 1973, p. 83). Sua expansão de Fourier é dada por (DIAMOND; SHURMAN, 2005, p. 5)

$$G_k(z) = 2\zeta(k) + 2 \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

onde $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ e $q \doteq q_1 = e^{2\pi i z}$. Defina $g_2(z) \doteq 60G_4(z)$ e $g_3(z) \doteq 140G_6(z)$.

^[58]Essencialmente, “ $f[\alpha]_k(\infty) = f(\alpha \cdot \infty)$ ”.

Exemplo 1.7.6 (Discriminante Modular). O **discriminante modular** é definido por

$$\Delta(z) \doteq g_2^3(z) - 27g_3^2(z).$$

Tal função é um exemplo de forma $\mathrm{SL}_2(\mathbb{Z})$ -cúspide de peso 12 (SERRE, 1973, p. 84). Notavelmente, Δ não se anula em $\mathbb{H}$ (SERRE, 1973, p. 88). Sua expansão de Fourier é dada por

$$\Delta(z) = (2\pi)^{12} \sum_{n \geq 1} \tau(n) q^n = q - 24q^2 + O(q^3),$$

onde $\tau(n)$ são inteiros^[59].

As formas modulares satisfazem as seguintes propriedades aritméticas:

- Proposição 1.7.7.** (i) (Soma) Se f e g são formas Γ -modulares (resp. Γ -cúspides) de peso k , $f + g$ é uma forma Γ -modular (resp. Γ -cúspide) de peso k .
- (ii) (Produto) Se f e g são formas Γ -modulares (resp. Γ -cúspides) de pesos k e l , respectivamente, fg é uma forma Γ -modular (resp. Γ -cúspide) de peso $k + l$.

Em particular, o espaço das formas Γ -modulares de peso k é um espaço vetorial, denotado por $\mathbb{M}_k(\Gamma)$, e o conjunto das formas Γ -cúspides de peso k é um subespaço, denotado por $\mathbb{S}_k(\Gamma)$. Estes espaços vetoriais têm dimensão finita: vale que (BRUINIER *et al.*, 2008, p. 12)

$$\dim(\mathbb{M}_k(\Gamma)) \leq \frac{k}{12} [\mathrm{SL}_2(\mathbb{Z}) : \Gamma] + 1.$$

Além disso, as somas diretas

$$\mathbb{M}(\Gamma) \doteq \bigoplus_{k=0}^{\infty} \mathbb{M}_k(\Gamma) \quad \text{e} \quad \mathbb{S}(\Gamma) \doteq \bigoplus_{k=0}^{\infty} \mathbb{S}_k(\Gamma)$$

são, respectivamente, uma $\mathbb{C}$ -álgebra graduada e um ideal homogêneo.

Exemplo 1.7.8 (Invariante Modular). O **invariante modular** é definido por

$$j(z) \doteq 1728 \frac{g_2^3(z)}{\Delta(z)}.$$

Apesar de ser holomorfa em $\mathbb{H}$ e invariante com relação à ação de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathbb{H}$, isto é,

$$j\left(\frac{az+b}{cz+d}\right) = j(z) \quad \forall z \in \mathbb{H}, \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

j não é uma forma modular^[60], pois não é holomorfa em ∞ : sua expansão de Fourier é^[61]

$$j(z) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n.$$

^[59]A função $n \mapsto \tau(n)$ é a **função τ de Ramanujan**. Conjectura-se que $\tau(n) \neq 0$ para todo n (LEHMER, 1943).

^[60]A função j é, na verdade, uma **função $\mathrm{SL}_2(\mathbb{Z})$ -modular** de peso 0, uma definição mais geral em que a condição de holomorphicidade em $\mathbb{H} \cup \{\infty\}$ é abrandada para meromorphicidade.

^[61]Notavelmente, todos os coeficientes c_n são inteiros (isto é garantido pelo fator 1728 na definição) e têm importantes conexões com as representações do grupo monstro, o maior grupo simples esporádico. Os coeficientes de Fourier da j são a sequência A000521 da OEIS (<<https://oeis.org/A000521>>).

Mesmo assim, j é sobrejetora sobre $\mathbb{C}$ e satisfaz (SERRE, 1973, p. 90)

$$j(z_1) = j(z_2) \iff \mathrm{SL}_2(\mathbb{Z}) \cdot z_1 = \mathrm{SL}_2(\mathbb{Z}) \cdot z_2.$$

1.7.1 Operadores de Hecke

Sejam Γ_1 e Γ_2 subgrupos de congruência. Como Γ_1 e Γ_2 também são subgrupos de $\mathrm{GL}_2^+(\mathbb{Q})$ (matrizes 2×2 de entradas racionais e determinante positivo), podemos, para cada $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, montar classes laterais duplas da forma $\Gamma_1 \alpha \Gamma_2 = \{\gamma_1 \alpha \gamma_2; \gamma_1 \in \Gamma_1 \text{ e } \gamma_2 \in \Gamma_2\} \in \Gamma_1 \backslash \mathrm{GL}_2^+(\mathbb{Q}) / \Gamma_2$.

Tome $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. O grupo Γ_1 age sobre $\Gamma_1 \alpha \Gamma_2$ por multiplicação à esquerda, donde podemos expressar esta classe lateral dupla em termos de finitas (DIAMOND; SHURMAN, 2005, p. 164, Lema 5.1.2) classes laterais disjuntas (órbitas da ação):

$$\Gamma_1 \alpha \Gamma_2 = \bigcup_{j=1}^n \Gamma_1 \beta_j \quad \text{com } \beta_1, \dots, \beta_n \in \alpha \Gamma_2.$$

Note que, se $f \in \mathbb{M}_k(\Gamma_1)$, temos que $f[\gamma]_k = f$, para todo $\gamma \in \Gamma_1$. Logo, se $\beta_j \in \mathrm{GL}_2^+(\mathbb{Q})$, “ $f[\Gamma_1 \beta_j]_k = f[\beta_j]_k$ ”. “Passando o colchete” na decomposição de $\Gamma_1 \alpha \Gamma_2$ acima, motivamos a

Definição 1.7.9. Sejam Γ_1 e Γ_2 subgrupos de congruência e $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Definimos o operador $[\Gamma_1 \alpha \Gamma_2]_k$, que age sobre $\mathbb{M}_k(\Gamma_1)$, por

$$f[\Gamma_1 \alpha \Gamma_2]_k = \sum_{j=1}^n f[\beta_j]_k \quad \text{onde } \Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2 = \{\beta_1, \dots, \beta_n\}.$$

Estes operadores convertem formas Γ_1 -modulares em formas Γ_2 -modulares e formas Γ_1 -cúspides em formas Γ_2 -cúspides (DIAMOND; SHURMAN, 2005, p. 165).

Quando $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, dois tipos importantes de operador colchete surgem^[62]:

Definição 1.7.10. • Seja $d \in \mathbb{N}$. Se $\mathrm{mdc}(d, N) = 1$, definimos o **operador diamante** $\langle d \rangle \doteq [\Gamma_1(N) \alpha \Gamma_1(N)]_k$, onde α é qualquer^[63] matriz de $\Gamma_0(N)$ com entrada inferior direita d ^[64]. Para $\mathrm{mdc}(d, N) \neq 1$, pomos $\langle d \rangle = 0$.

• Seja p primo. Definimos o operador $T_p \doteq [\Gamma_1(N) \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \Gamma_1(N)]_k$.

Estes operadores comutam entre si. Com isto, podemos estender o operador T_p indutivamente para potências de p por

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}$$

e para qualquer $n = p_1^{e_1} \dots p_r^{e_r}$ definindo $T_n = T_{p_1^{e_1}} \dots T_{p_r^{e_r}}$.

^[62]O nível N e o peso k ficam implícitos, determinados pelo contexto.

^[63]Note que $\Gamma_1(N)$ é o núcleo do mapa $\Gamma_0(N) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ que extrai a entrada inferior direita.

^[64]Como $\Gamma_1(N)$ é normal em $\Gamma_0(N)$, $\langle d \rangle = [\alpha]_k$, simplesmente.

Definição 1.7.11. A **Álgebra de Hecke** é a $\mathbb{C}$ -álgebra $\mathbb{T}$ gerada por $\{T_n, \langle n \rangle; n \in \mathbb{Z}_{>0}\}$. Seus elementos são os **operadores de Hecke**^[65].

1.7.1.1 Caracteres

Definição 1.7.12. Seja $N > 0$ inteiro. Um **caractere (de Dirichlet) módulo N** é um morfismo de grupos $\chi: \mathbb{Z}/N\mathbb{Z}^\times \rightarrow \mathbb{C}^\times$.

Proposição 1.7.13. Os caracteres módulo N formam um grupo multiplicativo $\widehat{\mathbb{Z}/N\mathbb{Z}^\times}$, chamado **grupo dual** de $\mathbb{Z}/N\mathbb{Z}^\times$. Além disso, $\widehat{\mathbb{Z}/N\mathbb{Z}^\times} \cong \mathbb{Z}/N\mathbb{Z}^\times$ (SERRE, 1973, p. 62, Proposição 2).

Em particular, existem finitos (mais especificamente, $\phi(N)$) caracteres módulo N . Denotamos a unidade de $\widehat{\mathbb{Z}/N\mathbb{Z}^\times}$ por $\mathbb{1}_N$ (ou $\mathbb{1}$, quando o N estiver subentendido).

Proposição 1.7.14 (Condições de Ortogonalidade).

$$\sum_{n \in \mathbb{Z}/N\mathbb{Z}^\times} \chi(n) = \begin{cases} \phi(N), & \chi = \mathbb{1} \\ 0, & \chi \neq \mathbb{1} \end{cases} \quad \text{e} \quad \sum_{\chi \in \widehat{\mathbb{Z}/N\mathbb{Z}^\times}} \chi(n) = \begin{cases} \phi(N), & n = 1 \\ 0, & n \neq 1 \end{cases}$$

(SERRE, 1973, p. 62, Proposição 4).

Podemos estender um caractere χ módulo N para $\mathbb{Z}$, fazendo $\chi(n) = 0$ sempre que $\text{mdc}(n, N) \neq 1$. Neste caso, mantemos as propriedades multiplicativas e as condições de ortogonalidade, mas o mapa resultante não será um morfismo de grupos.

Os caracteres módulo N interagem com as formas $\Gamma_1(N)$ -modulares do seguinte modo: para cada $\chi \in \widehat{\mathbb{Z}/N\mathbb{Z}^\times}$, considere o operador linear $\pi_\chi: \mathbb{M}_k(\Gamma_1(N)) \rightarrow \mathbb{M}_k(\Gamma_1(N))$ dado por

$$\pi_\chi = \frac{1}{\phi(N)} \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(d)^{-1} \langle d \rangle.$$

Estes operadores são comuns na Teoria de Representações (FULTON; HARRIS, 1991, Lecture 2) e satisfazem as seguintes propriedades:

- $\pi_\chi^2 = \pi_\chi$, isto é, π_χ é uma projeção.
- $\chi \neq \psi \implies \pi_\chi \circ \pi_\psi = 0$. Logo, as imagens de operadores distintos só se intersectam no 0.
- $\sum_{\chi \in \widehat{\mathbb{Z}/N\mathbb{Z}^\times}} \pi_\chi = 1$, isto é, as somas das imagens de todos os operadores geram $\mathbb{M}_k(\Gamma_1(N))$.

Denotando a imagem de π_χ por $\mathbb{M}_k(N, \chi)$, temos uma decomposição em subespaços

$$\mathbb{M}_k(\Gamma_1(N)) = \bigoplus_{\chi \in \widehat{\mathbb{Z}/N\mathbb{Z}^\times}} \mathbb{M}_k(N, \chi).$$

^[65]Em geral, usaremos este termo apenas para nos referir aos geradores de $\mathbb{T}$.

Explicitamente, estes espaços são dados por:

$$\mathbb{M}_k(N, \chi) = \{f \in \mathbb{M}_k(\Gamma_1(N)); \langle d \rangle f = \chi(d)f, \forall d \in \mathbb{Z}/N\mathbb{Z}^\times\}.$$

Definindo $\mathbb{S}_k(N, \chi) \doteq \mathbb{M}_k(N, \chi) \cap \mathbb{S}_k(\Gamma_1(N))$, temos uma decomposição análoga para o subespaço das formas cúspides:

$$\mathbb{S}_k(\Gamma_1(N)) = \bigoplus_{\chi \in \widehat{\mathbb{Z}/N\mathbb{Z}^\times}} \mathbb{S}_k(N, \chi).$$

Em particular,

$$\mathbb{M}_k(N, \mathbb{1}) = \mathbb{M}_k(\Gamma_0(N)) \quad \text{e} \quad \mathbb{S}_k(N, \mathbb{1}) = \mathbb{S}_k(\Gamma_0(N)).$$

1.7.1.2 Autoformas de Hecke

Definição 1.7.15. Seja $\mathcal{D}_1(N)$ um domínio fundamental^[66] da ação de $\Gamma_1(N)$ sobre $\mathbb{H}$. O **produto interno de Petersson** em $\mathbb{S}_k(\Gamma_1(N))$ é dado por

$$\langle f, g \rangle = \int_{\mathcal{D}_1(N)} f(z) \overline{g(z)} \text{Im}(z)^k d\mu(z),$$

onde $d\mu(x + iy) = \frac{dx dy}{y^2}$ é a medida hiperbólica^[67].

Os operadores $\langle n \rangle$ e T_n , para $\text{mdc}(n, N) = 1$, são normais com relação ao produto interno de Petersson. Em particular, existe uma base ortogonal de $\mathbb{S}_k(\Gamma_1(N))$ constituída de autovetores simultâneos de $\{\langle n \rangle, T_n; \text{mdc}(n, N) = 1\}$. Uma **autoforma (de Hecke)** é uma autoforma simultânea para $\langle n \rangle$ e T_n para todo $n \in \mathbb{Z}_{>0}$ tal que $a_1(f) = 1$ ^[68].

Teorema 1.7.16. Uma forma modular $f \in \mathbb{M}_k(N, \chi)$ é uma autoforma se, e somente se,

- (i) $a_1(f) = 1$;
- (ii) $a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - \chi(p)p^{k-1}a_{p^{r-2}}(f)$, para todo p primo e $r \geq 2$;
- (iii) $a_{mn}(f) = a_m(f)a_n(f)$ sempre que $\text{mdc}(m, n) = 1$

(DIAMOND; SHURMAN, 2005, p. 198, Proposição 5.8.5).

^[66] Um **domínio fundamental** da ação de um grupo sobre um espaço topológico é um conjunto conexo de únicos representantes para cada órbita.

^[67] $\mathbb{H}$ possui estrutura natural de espaço hiperbólico. Portanto, esta medida funciona bem aqui: em particular, é invariante pelo grupo de automorfismos de $\mathbb{H}$, que é $\text{PGL}_2^+(\mathbb{R})$, o grupo das matrizes 2×2 de entradas reais e determinante positivo, descontadas matrizes múltiplas (que agem da mesma forma sobre $\mathbb{H}$).

^[68] Estamos pedindo um pouco mais do que ser autovetor simultâneo dos $\{\langle n \rangle, T_n; \text{mdc}(n, N) = 1\}$. Referimos o leitor interessado a (DIAMOND; SHURMAN, 2005, p. 195, Seção 5.8) para uma justificativa detalhada.

1.8 Tópicos de L -funções

Grosso modo, uma **L -função** é uma série da forma $L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, onde $a_n \in \mathbb{C}$ e L satisfaz algumas propriedades como convergir num semiplano complexo e possuir extensão ao menos meromorfa para todo o plano complexo^[69].

Exemplo 1.8.1 (L -funções de Dirichlet). Seja $N > 0$ inteiro e χ um caractere módulo N . A L -função de Dirichlet de χ é definida por

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \operatorname{Re}(s) > 1$$

(o caso $\chi = \mathbb{1}_1$ é a função ζ de Riemann).

Estas L -funções estão relacionadas a outro dos grandes problemas em aberto da Matemática (e outro problema de 1 milhão de dólares!): a Hipótese de Riemann.

Conjectura 1.8.2 (Hipótese de Riemann Generalizada). Se $L(s, \chi) = 0$ e s não é um inteiro, então $\operatorname{Re}(s) = \frac{1}{2}$ (o caso $\chi = \mathbb{1}_1$ é a Hipótese de Riemann propriamente dita)^[70].

Exemplo 1.8.3 (L -funções de formas $\Gamma_1(N)$ -cúspides). Seja $f = \sum_{n=1}^{\infty} a_n(f)q^n \in \mathbb{S}_k(\Gamma_1(N))$ uma forma $\Gamma_1(N)$ -cúspide. A L -função de f é definida por

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}, \quad \operatorname{Re}(s) > \frac{k}{2} + 1.$$

Além das propriedades básicas, queremos que uma L -função possua uma equação funcional que relaciona seus valores em um semiplano esquerdo com um semiplano direito do plano complexo. As L -funções de certas formas modulares possuem tal propriedade^[71]:

A transformada de Mellin de uma forma cúspide f é dada por (DIAMOND; SHURMAN, 2005, p. 204, Proposição 5.10.1)

$$\mathcal{M}(s, f) \doteq \int_0^{\infty} f(it)t^{s-1} dt = \frac{1}{(2\pi)^s} \Gamma(s) L(s, f),$$

onde $\Gamma(s) = \int_0^{\infty} t^{s-1} e^{-t} dt$. Defina $\Lambda(s, f) = N^{s/2} \mathcal{M}(s, f)$.

^[69]Não há uma definição precisa para o termo “ L -função”. Isto porque tais funções normalmente aparecem associadas a outros objetos (*e.g.* caracteres, formas modulares, curvas elípticas) e, por terem comportamentos tão parecidos, acabam levando o mesmo nome. Veja Bruin (2012) para mais informações.

^[70]Veja Bombieri (2000) para a descrição oficial da Hipótese de Riemann como Problema do Milênio e Sarnak (2004) para uma introdução sucinta. Uma introdução mais completa pode ser encontrada em Apostol (1976).

^[71]As L -funções de Dirichlet, e em particular a função ζ de Riemann, também possuem tais equações funcionais, conforme as referências citadas.

Proposição 1.8.4 (Hecke). Se $f \in \mathbb{S}_2(\Gamma_0(N))$ é uma autoforma, então

$$\Lambda(s, f) = w\Lambda(2-s, f),$$

com $w \in \{\pm 1\}$.^[72] Em particular, $L(s, f)$ admite uma extensão analítica para todo o plano complexo (MIYAKE, 2006, p. 122, Corolário 4.3.7).^[73]

Outra propriedade que gostaríamos que uma L -função possuísse é poder ser expressa por um **produto de Euler**, isto é, que pudéssemos escrever $L(s)$ como um produto infinito

$$L(s) = \prod_{p \text{ primo}} L_p(s).$$

Ilustraremos esta propriedade com o caso mais simples de L -função que é a função ζ de Riemann, de onde se originou o produto de Euler.

Proposição 1.8.5. Para todo $s \in \{z \in \mathbb{C}, \operatorname{Re}(z) > 1\}$, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}}$.

A ideia por trás desta fórmula é a mesma por trás do Crivo de Eratóstenes: cada primo p elimina todos os números dos quais é o menor divisor primo. Considere $2^{-s}\zeta(s)$. Esta é a soma de todos os termos de ζ cujo menor divisor primo é 2. Assim, eliminando-os, $(1-2^{-s})\zeta(s)$ é constituído apenas dos termos que não são divisíveis por 2. Multiplicar esta soma por $(1-3^{-s})$ elimina os termos múltiplos de 3 (os múltiplos de 6 já foram eliminados no passo anterior – já que 2 é o menor divisor primo destes), e assim por diante. Logo, $\prod_{p \text{ primo}} (1-p^{-s})\zeta(s) = 1$.^[74]

Seja $f \in \mathbb{S}_k(N, \chi)$ uma autoforma. Então, $L(s, f)$ também pode ser expressa como um produto de Euler:

Proposição 1.8.6. Para todo $s \in \left\{z \in \mathbb{C}, \operatorname{Re}(z) > 1 + \frac{k}{2}\right\}$,

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s} = \prod_{p \text{ primo}} \frac{1}{1 - a_p(f)p^{-s} + \chi(p)p^{k-1-2s}}.$$

Vamos tentar interpretar esta fórmula à luz da discussão acima (para simplificar a notação, escreveremos a_n em vez de $a_n(f)$): considere $(a_2 2^{-s} - \chi(2) 2^{k-1-2s})L(s, f)$. Afirmamos que

$$(a_2 2^{-s} - \chi(2) 2^{k-1-2s})L(s, f) = \sum_{2|n} \frac{a_n}{n^s}.$$

^[72]O sinal desta equação, chamado **root number** de f , é o autovalor de f como autovetor da **involução de Atkin-Lehner**, o operador $W_N: \mathbb{S}_2(\Gamma_0(N)) \rightarrow \mathbb{S}_2(\Gamma_0(N))$ dado por $f \mapsto -f \left[\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix} \right]_2$ (DIAMOND; SHURMAN, 2005, p. 204).

^[73]Veja também Lang (1986), Capítulos 13 (para a prova original de Hecke) e 14 (para a prova de Tate).

^[74]Claro que este procedimento precisa ser formalizado, mas este é o raciocínio que levou Euler a descobrir esta fórmula. Refira a Apostol (1976) para mais detalhes.

Rearranjando formalmente os termos da série^[75]:

$$\begin{aligned}
 (a_2 2^{-s} - \chi(2) 2^{k-1-2s}) \sum_{n=1}^{\infty} a_n n^{-s} &= (a_2 2^{-s} - \chi(2) 2^{k-1-2s}) \sum_{2 \nmid n'} \sum_{r=0}^{\infty} a_{2^r n'} (2^r n')^{-s} \\
 &= \left(\sum_{2 \nmid n'} a_{n'} (n')^{-s} \right) \left(\sum_{r=0}^{\infty} a_2 a_{2^r} \cdot 2^{-(r+1)s} - \sum_{r=0}^{\infty} \chi(2) 2^{k-1} a_{2^r} \cdot 2^{-(r+2)s} \right) \\
 &= \left(\sum_{2 \nmid n'} a_{n'} (n')^{-s} \right) \left(a_2 2^{-rs} + \sum_{r=2}^{\infty} \underbrace{(a_2 a_{2^{r-1}} - \chi(2) 2^{k-1} a_{2^{r-2}})}_{= a_{2^r}} 2^{-rs} \right) = \sum_{2|n} \frac{a_n}{n^s}
 \end{aligned}$$

Logo, $(1 - a_2 2^{-s} + \chi(2) 2^{k-1-2s}) L(s, f) = \sum_{2 \nmid n} \frac{a_n}{n^s}$. Adaptando este raciocínio, multiplicar a soma restante por $(1 - a_3 3^{-s} + \chi(3) 3^{k-1-2s})$ elimina todos os termos múltiplos de 3 (e, como antes, os múltiplos de 6 já foram eliminados), e assim por diante, à maneira de Eratóstenes. Logo,

$$\prod_{p \text{ primo}} (1 - a_p(f) p^{-s} + \chi(p) p^{k-1-2s}) L(s, f) = 1.$$

^[75]Infelizmente a recorrência que define a_{p^n} não é tão simples quanto a recorrência $p^n = p \cdot p^{n-1}$!

CURVAS ELÍPTICAS

2.1 Cúbicas de Weierstrass e curvas elípticas

Seja K um corpo^[76]. Uma **cúbica** sobre K é uma curva algébrica C definida por um polinômio cúbico com coeficientes em K . Estamos interessados especialmente em cúbicas dadas por uma equação da forma

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \quad (2.1)$$

chamadas **cúbicas de Weierstrass**. Neste caso, note que o único ponto no infinito de C é $O \doteq (0 : 1 : 0)$. Portanto, não perdemos muito em considerar a versão afim desta equação:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (2.2)$$

A partir da equação acima, definimos as seguintes constantes:

$$\begin{aligned} b_2 &\doteq a_1^2 + 4a_4, & b_4 &\doteq a_1a_3 + 2a_4, & b_6 &\doteq a_3^2 + 4a_6, \\ b_8 &\doteq a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2. \end{aligned}$$

Assim, o **discriminante** da equação (2.2) é definido por

$$\Delta \doteq -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Definição 2.1.1. Uma **curva elíptica** sobre K é uma cúbica não-singular dada por uma equação de Weierstrass, ou equivalentemente, dada por uma equação de Weierstrass com $\Delta \neq 0$.

^[76]N.B.: De agora em diante todas as curvas algébricas (afins ou projetivas) mencionadas são planas, a menos de menção em contrário.

Exemplo 2.1.2. Para exemplificar o conceito, as figuras a seguir mostram a parte afim de duas curvas elípticas reais. O ponto O , como vimos, é pensado como o topo do eixo vertical:

Figura 1 – Exemplos de curvas elípticas reais

Fonte: Elaborada pelo autor.

Uma outra definição comumente encontrada para curvas elípticas é:

Definição 2.1.3. Uma **curva elíptica** sobre K é uma curva não-singular de gênero 1 com um ponto K -racional.

Proposição 2.1.4. As definições 2.1.1 e 2.1.3 são equivalentes.

Prova. Se C é uma cúbica não-singular dada por uma equação de Weierstrass, é fácil ver que $g = 1$. Reciprocamente, se C é uma curva não-singular de gênero 1 com um ponto K -racional P , considere os espaços de Riemann–Roch $L(nP)$. Pelo Teorema de Riemann–Roch (Teorema 1.1.4), $\ell(nP) = n$. Assim, existem $x, y \in K(E)$ tais que $\{1, x\}$ é uma base de $L(2P)$ ($\implies \text{ord}_P(x) = -2$) e $\{1, x, y\}$ é uma base de $L(3P)$ ($\implies \text{ord}_P(y) = -3$). Note que

$$1, x, y, xy, x^2, x^3, y^2 \in L(6P),$$

mas, como $\ell(6P) = 6$, existe uma combinação linear não-trivial

$$\alpha_1 + \alpha_2 x + \alpha_3 y + \alpha_4 xy + \alpha_5 x^2 + \alpha_6 x^3 + \alpha_7 y^2 = 0,$$

que pode ser transformada numa equação de Weierstrass. ■

Voltando ao caso geral, defina também as constantes

$$c_4 \doteq b_2^2 - 24b_4 \quad \text{e} \quad c_6 \doteq -b_2^3 + 36b_2b_4 - 216b_6.$$

Em termos destas constantes, o discriminante de uma cúbica de Weierstrass é dado por

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

Se uma cúbica de Weierstrass C é singular, $\Delta = 0$. Como C é irredutível, pelo Teorema de Bézout (Teorema 1.1.1), existe um único ponto singular P_0 ^[77]. O ponto no infinito O nunca é singular (pois não anula a derivada em z do polinômio de Weierstrass). Logo, P_0 está na parte afim e, por uma translação^[78], podemos supor que seja o $(0, 0)$. Neste caso, se

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

é o polinômio de Weierstrass que define C , isto quer dizer que

$$f(0, 0) = 0, \quad \frac{\partial f}{\partial x}(0, 0) = 0 \quad \text{e} \quad \frac{\partial f}{\partial y}(0, 0) = 0,$$

ou seja, f é da forma

$$f(x, y) = y^2 + a_1xy - x^3 - a_2x^2 = (y - \alpha_1x)(y - \alpha_2x) - x^3,$$

para alguns α_1 e α_2 definidos, *a priori*, sobre $\bar{K}$. As retas $y = \alpha_1x$ e $y = \alpha_2x$ são as retas tangentes a C em P_0 . Se estas retas forem distintas, C é uma **cúbica nodal** e, se forem iguais, C é uma **cúbica cuspidal**^[79]. Sobre $\mathbb{R}$, estas possuem as respectivas formas

Figura 2 – Traço real das cúbicas planas singulares

Fonte: [Diamond e Shurman \(2005, p. 314\)](#).

Observe que $c_4 = (\alpha_1 - \alpha_2)^4$. Assim, obtemos uma maneira mais “intrínseca” de classificar cúbicas de Weierstrass:

^[77]Se existissem dois pontos singulares P_0 e P_1 , a reta L passando por eles intersectaria C com multiplicidade 2 em cada um deles. Pelo Teorema de Bézout,

$$4 = (C, L)_{P_0} + (C, L)_{P_1} = \deg(C) \deg(L) = 3,$$

uma contradição.

^[78]Translações são isomorfismos que preservam c_4 e c_6 , e portanto Δ , como veremos logo adiante.

^[79]Em característica 3 há duas cúbicas cuspidais, a menos de isomorfismo. Logo, neste cenário, o termo “cúbica cuspidal” se refere a ambos os casos.

Proposição 2.1.5. Seja C uma cúbica de Weierstrass. Então,

- C é uma curva elíptica se, e somente se, $\Delta \neq 0$;
- C é uma cúbica nodal se, e somente se, $\Delta = 0$ e $c_4 \neq 0$;
- C é uma cúbica cuspidal se, e somente se, $\Delta = 0$ e $c_4 = 0$.

Um dos motivos por que estamos interessados em curvas elípticas é sua estrutura de grupo abeliano. A regra da soma, chamada **lei da corda-tangente**, é definida por

Se P, Q e R são colineares, então $P + Q + R = O$.

Esquemáticamente,

Figura 3 – Lei da corda-tangente

Fonte: Adaptada de [Diamond e Shurman \(2005, p. 253\)](#).

A única propriedade de grupo que não é imediata é a associatividade. Apesar de ser possível demonstrá-la diretamente, a maneira mais comum (e mais elegante que a primeira) de fazê-lo é recorrer ao seguinte resultado:

Teorema 2.1.6 (Cayley–Bacharach). Se uma cúbica C_1 intersecta uma cúbica irredutível C em 9 pontos não necessariamente distintos (pelo Teorema de Bézout) e outra cúbica C_2 intersecta C em 8 destes pontos, então C_2 também passa pelo nono ponto.

Prova. Usando a notação de ciclos de intersecção, escreva

$$C \cdot C_1 = \sum_{i=1}^9 P_i \quad \text{e} \quad C \cdot C_2 = \sum_{i=1}^8 P_i + Q.$$

Suponha que $Q \neq P_9$. Neste caso, podemos tomar uma reta L passando por P_9 que não passa por Q . Sejam R e S os outros pontos em $L \cap C$, possivelmente iguais. Então^[80],

$$LC_2 \cdot C = C_1 \cdot C + Q + R + S \implies LC_2 \cdot C \leq C_1 \cdot C.$$

Pelo Teorema de Max Noether (Teorema 1.1.2), há uma reta L' tal que $L' \cdot C = Q + R + S$. Como L e L' coincidem em 3 pontos, $L = L'$, o que implicaria que $Q = P_9$, uma contradição. ■

Corolário 2.1.7. Uma curva elíptica E , com a lei da corda-tangente, é um grupo abeliano.

Prova. A operação está bem-definida pelo Teorema de Bézout e, como dois pontos definem a mesma reta independente da ordem em que são tomados, a operação é comutativa.

Note que O é o elemento neutro do grupo: de fato, seja R o terceiro ponto em que a reta passando por P e O intersecta E . Logo, a reta definida por R e O é esta mesma reta, donde $-R = P = P + O$. Também é fácil ver que R é o inverso de P , já que $P + R + O = P + R = O$.

Para a associatividade, sejam $P, Q, R \in E$ para os quais desejamos mostrar que $P + (Q + R) = (P + Q) + R$ e considere as seguintes retas e pontos sucessivamente obtidos a partir destes:

$$\begin{array}{ll} L_1 \cdot E = P + Q + S' & M_1 \cdot E = O + S' + S \\ L_2 \cdot E = S + R + T' & M_2 \cdot E = Q + R + U' \\ L_3 \cdot E = O + U' + U & M_3 \cdot E = P + U + T'' \end{array}$$

Portanto, o que queremos mostrar é que $T' = T''$, mas isto segue do Teorema de Cayley–Bacharach para $C = E$, $C_1 = L_1L_2L_3$ e $C_2 = M_1M_2M_3$. ■

É possível definir, da mesma forma, a lei da corda-tangente para o subconjunto (aberto) C_{ns} dos pontos não-singulares de uma cúbica de Weierstrass singular C .

Proposição 2.1.8. Seja $C: (y - \alpha_1 x)(y - \alpha_2 x) = x^3$ uma cúbica de Weierstrass irreduzível.

- Se $\alpha_1, \alpha_2 \in K$,

$$(C_{\text{ns}}(K), +) \cong \begin{cases} (K^\times, \cdot), & \text{se } C \text{ é nodal} \\ (K, +), & \text{se } C \text{ é cuspidal;} \end{cases} \text{[81]}$$

- Senão, seja $K' = K(\alpha_1) = K(\alpha_2)$. Note que α_1 e α_2 são as duas raízes do polinômio $p(t) \doteq t^2 + a_1 t - a_2 \in K[t]$.

^[80]Aqui, abusamos um pouco da notação, denotado pelo produto de duas curvas a curva obtida pelo produto dos polinômios que definem cada fator. Este e outros abusos de notação envolvendo a curva e o polinômio que o geram serão comuns ao longo do texto (talvez até já tenham acontecido antes!).

^[81]Um pequeno truque para lembrar qual grupo corresponde a cada cúbica singular é desenhar a cúbica, as retas tangentes à singularidades, e uma reta vertical passando pela singularidade. No caso da cúbica nodal, as retas formarão um asterisco (*) e, no caso da cúbica cuspidal, um sinal de mais (+)!

- Se C é nodal, p é irredutível e $[K' : K] = 2$. Seja $\text{Gal}(K', K) = \langle \sigma \rangle$. Então, $(C_{\text{ns}}(K), +)$ é isomorfo ao subgrupo multiplicativo $\{a \in K'; a\sigma(a) = 1\}$; ^[82]
- Se C é cuspidal (apenas em característica 2), $(C_{\text{ns}}(K'), +) \cong (K', +)$.

(HUSEMÖLLER, 2004, p. 81, Teorema 7.2).

Definição 2.1.9. Sejam E_1 e E_2 duas curvas elípticas sobre K . Uma **isogenia** definida sobre K é um mapa $\varphi: E_1 \rightarrow E_2$ que é tanto um morfismo de curvas algébricas quanto um morfismo de grupos. Uma isogenia inversível por outra isogenia é um **isomorfismo**.

Desta forma, uma isogenia é um mapa que leva em consideração ambas as estruturas de uma curva elíptica: a de curva algébrica e a de grupo abeliano.

Exemplo 2.1.10 (Multiplicação por inteiro). Seja E uma curva elíptica e $N \in \mathbb{Z}$. A isogenia de multiplicação por N é dada por

$$[N]: E \rightarrow E, \quad [N](P) = \begin{cases} \underbrace{P + \dots + P}_{N \text{ vezes}} & N \geq 0 \\ -(\underbrace{P + \dots + P}_{|N| \text{ vezes}}) & N < 0 \end{cases} \quad \text{com } N \in \mathbb{Z}$$

(SILVERMAN, 2009, p. 67, Exemplo III.4.1). Se $N > 0$, o núcleo de $[N]$ é o subgrupo dos pontos de N -torção de E , que denotamos por $E[N]$.

Teorema 2.1.11 (Estrutura da p -torção). Seja E uma curva elíptica sobre K e p primo. Se $\text{car}(K) = 0$, então

$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/p^e\mathbb{Z}, \quad \forall e \geq 1.$$

Se $\text{car}(K) = p$, então uma das duas opções ocorre para todo $e \geq 1$:

$$E[p^e] \cong \{O\} \quad \text{ou} \quad E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$$

(SILVERMAN, 2009, p. 86, Corolário III.6.4).

Proposição 2.1.12. Seja $\varphi: E \rightarrow E'$ um isomorfismo de curvas elípticas. Visto como uma mudança de coordenadas, φ é da forma

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + su^2x' + t \end{cases},$$

com $r, s, t \in K$ e $u \in K^\times$ (SILVERMAN, 2009, p. 44).

Em particular, um isomorfismo $\varphi: E \rightarrow E'$ na forma acima faz com que ^[83]:

$$c_4 = u^4c'_4, \quad c_6 = u^6c'_6, \quad \Delta = u^{12}\Delta'.$$

^[82]Este é o núcleo da **norma** $N_{K'/K}: (K')^\times \rightarrow (K')^\times, a \mapsto a\sigma(a)$.

^[83]Além disso, se $r = s = t = 0$, $a_i = u^i a'_i$ para todo $i \in \{1, \dots, 6\}$ e $b_j = u^j b'_j$ para todo $j \in \{2, 4, 6, 8\}$, o que explica os índices destes coeficientes.

Definição 2.1.13. Definimos o *j*-invariante de uma curva elíptica E por

$$j(E) \doteq \frac{c_4^3}{\Delta}.$$

Se K é um corpo de característica diferente de 2 ou 3^[84], uma mudança de coordenadas adequada coloca a equação de Weierstrass na forma mais simples^[85]

$$y^2 = x^3 + ax + b. \quad (2.3)$$

Nesta forma, o discriminante e o *j*-invariante de uma curva elíptica passam a ser dados por

$$\Delta = -16(4a^3 + 27b^2) \quad \text{e} \quad j = 1728 \frac{4a^3}{4a^3 + 27b^2} = -1728 \frac{(4a)^3}{\Delta},$$

e um isomorfismo $\varphi: E \rightarrow E'$ entre duas curvas elípticas nesta forma é dado por

$$\begin{cases} x = u^2 x' \\ y = u^3 y' \end{cases},$$

com $u \in K^\times$.

A seguinte propriedade mostra que o *j*-invariante não é assim chamado à toa:

Proposição 2.1.14. Duas curvas elípticas E e E' sobre K são isomorfas sobre $\bar{K}$ se, e somente se, $j(E) = j(E')$.

Ideias da Prova. (com $\text{car}(K) \notin \{2, 3\}$). A implicação direta é imediata, pela forma geral do isomorfismo. Para a recíproca, note que $j(E) = j(E') \implies a^3(b')^2 = (a')^3b^2$. Se $a \neq 0$, tome $u = (a'/a)^{1/4}$ (que existe, pois $\bar{K}$ é algebricamente fechado). Se não, tome $u = (b'/b)^{1/6}$, pois a condição $\Delta \neq 0$ garante que a e b não podem ser ambos nulos. $\square$

Observação 2.1.15. Duas curvas elípticas com mesmo *j*-invariante definidas sobre um corpo K não algebricamente fechado podem não ser isomorfas sobre K . Considere $y^2 = x^3 - 25x$ e $y^2 = x^3 - 4x$ sobre $\mathbb{Q}$. Ambas têm *j*-invariante 1728, mas a primeira curva tem infinitos pontos racionais e a segunda só tem 4 (WASHINGTON, 2008, p. 224, Exemplos 8.7 e 8.8).

Nas seções e capítulos seguintes, apresentamos particularidades das curvas elípticas definidas sobre diversos corpos.

^[84]Em característica 2, não é possível eliminar os termos lineares em y , enquanto que, em característica 3, se $j(E) \neq 0$, não é possível eliminar o termo em x^2 . Estes casos devem ser tratados separadamente e não nos deteremos neles aqui. Referimos o leitor interessado a (SILVERMAN, 2009, Apêndice A).

^[85]Explicitamente, $a \doteq -27c_4$ e $b \doteq -54c_6$.

2.2 Redução de curvas elípticas módulo valorizações

Seja (K, v) um corpo de números ou o completamento de um destes com relação a um lugar não-arquimediano, munido de uma valorização v , e C uma cúbica de Weierstrass sobre K . Por um isomorfismo $(x, y) = (u^2x', u^3y')$ adequado, podemos supor que os coeficientes de C estão em $\mathcal{O}_v$ (dizemos que C está na forma **v -integral**) e, portanto, reduzi-los módulo v . Como é a redução $\tilde{C}$ de C módulo v ?

Note que uma curva elíptica pode reduzir módulo v para uma cúbica singular: basta que seu discriminante esteja no ideal maximal $\mathfrak{m}_v$. No caso $K = \mathbb{Q}$ e $v = v_p$, isto é o mesmo que o discriminante ser divisível por p . Gostaríamos que a redução de uma curva elíptica continuasse a ser uma curva elíptica. Por isso, para reduzir módulo v , escolhemos um modelo de E (isto é, uma curva elíptica isomorfa a E) tal que $v(\Delta(E))$ seja o menor possível. Defina

$$v(E) = \min\{v(\Delta(E')); E' \text{ é } v\text{-integral e } E' \cong E\}$$

(que é não negativo, pois $\Delta(E') \in \mathcal{O}_v$ para todo E' nestas condições). Uma curva elíptica E' é um **modelo v -minimal** de E se $v(\Delta(E')) = v(E)$.

Isomorfismos fazem $v(\Delta)$ variar em um múltiplos de 12 (Proposição 2.1.12) e, similarmente, $v(c_4)$ e $v(c_6)$ variam em múltiplos de 4 e 6, respectivamente. Logo,

$$\text{se } v(c_4) < 4 \text{ ou } v(c_6) < 6 \text{ ou } v(\Delta) < 12, \text{ então } E \text{ é um modelo } v\text{-minimal}, \quad (2.4)$$

e vale a recíproca.^[86]

Suponha momentaneamente que $K = \mathbb{Q}$. Podemos considerar um modelo minimal simultâneo para todos os primos p : Definimos o **discriminante minimal global** de E por

$$\Delta_{\min}(E) = \prod_{p \text{ primo}} p^{v_p(E)}.$$

Note que este produto é finito pois $p \nmid \Delta(E) \implies v_p(E) = 0$. Uma curva elíptica integral E' isomorfa a E tal que $\Delta(E') = \Delta_{\min}(E)$ é chamada **modelo minimal global** de E ^[87].

Proposição 2.2.1. Toda curva elíptica E admite um modelo minimal global. Além disso, dois modelos minimais globais E' e E'' são isomorfos com $c'_4 = c''_4$ e $\Delta' = \Delta''$.

Prova. Como $E' \cong E \cong E''$, existe um isomorfismo $E' \rightarrow E''$ dado por

$$\begin{cases} x' = u^2x'' + r \\ y' = u^3y'' + su^2x'' + t \end{cases},$$

^[86]Mais especificamente, se E é um modelo v -minimal, então $v(c_4) < 4$ ou $v(\Delta) < 12$. De fato, se $v(c_4) \geq 4$ e $v(\Delta) \geq 12$, então $c_4 = \pi^4 c'_4$ e $\Delta = \pi^{12} \Delta'$, onde π é um parâmetro uniformizador de $\mathcal{O}_v$. Logo, $c_6 = \pi^6 c'_6$ (aqui, estamos usando que $\text{car}(K) \neq 2, 3$). Considerando o isomorfismo $(x, y) = (\pi^2 x', \pi^3 y')$, obtemos uma curva elíptica E' v -integral com $v(\Delta(E')) < v(\Delta(E))$. Logo, E não é v -minimal.

^[87]Se $K = \mathbb{K}$ é um corpo de números, podemos definir analogamente o discriminante minimal global de E por $\mathfrak{D}_{\min}(E) = \prod_{\mathfrak{p} \text{ primo}} \mathfrak{p}^{v_{\mathfrak{p}}(E)}$, que passa a ser um ideal de $\mathcal{O}_{\mathbb{K}}$, em vez de um inteiro.

com $r, s, t \in \mathbb{Q}$ e $u \in \mathbb{Q}^\times$. Como $\Delta(E') = \Delta_{\min}(E) = \Delta(E'') = \Delta(E')/u^{12}$, temos que $u = \pm 1$, donde $c_4'' = c_4'/u^4 = c_4'$. ■

Podemos, portanto, supor que as curvas elípticas sobre $\mathbb{Q}$ estão em um modelo minimal global sempre que necessário. A vantagem deste modelo é que minimizamos simultaneamente a divisibilidade do discriminante da curva por potências de primos.

De volta ao caso geral, classificamos as possibilidades para a redução de E módulo v :

Definição 2.2.2. Seja E uma curva elíptica. A redução de E módulo v é:

- **Boa** (não-singular) se $\tilde{E}$ é uma curva elíptica ($\iff v(\Delta(E)) = 0$). Além disso, também denominamos a redução como
 - **ordinária**, se $\tilde{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$;
 - **supersingular**, se $\tilde{E}[p] = 0$ ^[88].
- **Má** (singular) se $\tilde{E}$ é singular. Além disso, também denominamos a redução como
 - **multiplicativa**, se $\tilde{E}$ é nodal ($\iff v(\Delta(E)) > 0, v(c_4) = 0$). Diz-se, ainda, que a redução multiplicativa é *split* se as duas retas tangentes a $\tilde{E}$ na singularidade estão definidas sobre o corpo residual k_v ;
 - **aditiva**, se $\tilde{E}$ é cuspidal ($\iff v(\Delta(E)) > 0, v(c_4) > 0$)^[89];

Também dizemos que E , de modo geral, tem redução

- **estável**, se E tem boa redução em todo lugar não-arquimediano v ;
- **semi-estável**, se a redução de E módulo cada v é ou boa ou multiplicativa;
- **instável**, se E tem redução aditiva em algum lugar não-arquimediano v .^[90]

Observação 2.2.3. A redução de E independe do modelo v -minimal escolhido.

Ideias da Prova. Sejam $E' \cong E''$ dois modelos v -minimais, onde o isomorfismo é da forma indicada na Proposição 2.1.12. Como $v(\Delta') = v(\Delta'')$ e $u^{12}\Delta' = \Delta$, temos que $u \in \mathcal{O}_v^\times$. Resta mostrar que $r, s, t \in \mathcal{O}_v$. Para isto, recorremos a fórmulas que relacionam os coeficientes a'_i e b'_j de E' com os a''_i e b''_j de E'' (SILVERMAN, 2009, p. 45) e, primeiro, observamos as expressões da forma $b''_j - b'_j$, que serão dadas em termos de r , e que mostram ser impossível que $v(r) < 0$, isto é, $r \in \mathcal{O}_v$. Em seguida, expressões da forma $\pm a''_i - a'_i$, analisadas de maneira análoga, mostram que $s, t \in \mathcal{O}_v$. Logo, o isomorfismo se reduz módulo v , donde $\tilde{E}' \cong \tilde{E}''$. □

^[88]Estas são as duas únicas possibilidades para $\tilde{E}[p]$, pelo Teorema 2.1.11.

^[89]Os nomes das reduções más vêm da estrutura de grupo da parte não singular de $\tilde{E}$ (Proposição 2.1.8).

^[90]Algumas referências usam estável, semi-estável e instável ora como sinônimos de, respectivamente, redução boa, multiplicativa e aditiva em um certo lugar e ora da mesma maneira que definimos. Para evitar confusão, resolvemos diferenciar os significados destas duas classes de termos.

Ilustraremos os tipos de redução que apresentamos acima com exemplos (todas as curvas elípticas a seguir estão em modelos minimais adequados, salvo menção em contrário):

Exemplo 2.2.4. A curva elíptica $E: y^2 + xy + y = x^3 + x^2$ sobre $\mathbb{Q}$ (LMFDB 30.a8) tem discriminante $\Delta = -2160 = -2^4 \cdot 3^3 \cdot 5$ e $c_4 = -47$. A redução de E é semi-estável, sendo

- Multiplicativa não-*split* em $p = 2$ e 5 ;
- Multiplicativa *split* em $p = 3$;
- Boa^[91] em $p \geq 7$.

Exemplo 2.2.5. A curva elíptica $E: y^2 + \sqrt{6}xy + (\sqrt{6} + 1)y = x^3 + (1 - \sqrt{6})x^2 - (3\sqrt{6} + 1)x - (2\sqrt{6} + 1)$ sobre $\mathbb{Q}(\sqrt{6})$ (LMFDB 1.1-a1) tem discriminante minimal global (cf. nota [87]) $\mathfrak{D}_{\min} = (1)$, donde a redução de E é estável.

Observação 2.2.6. Nenhuma curva elíptica sobre $\mathbb{Q}$ tem redução estável (boa em todos os primos). Seja $E/\mathbb{Q}$ num modelo minimal global e suponha que $\Delta(E) = \pm 1$. Então, a_1 é ímpar, pois se fosse par, teríamos que $b_2 \equiv 0 \pmod{4}$ e $b_4 \equiv 0 \pmod{2}$. Logo,

$$\Delta = \pm 1 = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \equiv 5b_6^2 \pmod{8},$$

o que não pode ser. Sendo a_1 ímpar, $c_4 \equiv a_1^4 \equiv 1 \pmod{8}$. Escreva $c_4 = u \pm 12$ (o mesmo sinal de Δ). Então,

$$c_4^3 - c_6^2 = \pm 1728 \implies c_6^2 = u(u^2 \pm 36u + 432) \equiv 0 \pmod{8}$$

Se u não for um quadrado, podemos escrever $u = p_1 \dots p_n u'$ onde p_i são primos distintos e u' é um quadrado. Como o produto no segundo membro é um quadrado, $p_1 \mid u \implies p_1 \mid (u^2 \pm 36u + 432) \implies p_1 \mid 432 \implies p_1 = 2$ ou 3 . Note que u é ímpar, pois c_4 o é. Logo, $n = 1$ e $p_1 = 3$, ou seja, $u = \square$ ou $3\square$. Porém, os resíduos quadráticos módulo 8 são 0, 1 e 4. Como $u \equiv 5 \pmod{8}$, nenhum destes casos pode ocorrer, obtendo-se uma contradição.

Exemplo 2.2.7. A curva elíptica $E: y^2 = x^3 + x + 2$ sobre $\mathbb{Q}$ (LMFDB 56.a4) tem discriminante $\Delta = -1792 = -2^8 \cdot 7$ e $c_4 = -48$. A redução de E é instável, sendo

- Aditiva em $p = 2$;
- Multiplicativa não-*split* em $p = 7$;
- Boa nos demais primos.

^[91]Por enquanto não temos nenhuma maneira prática de distinguir reduções boas ordinárias e supersingulares. No capítulo seguinte apresentaremos um critério que permite esta distinção (Proposição 3.2.5).

Exemplo 2.2.8. (SILVERMAN, 2009, p. 186, Exemplo VII.1.2). Considere a curva elíptica $E: y^2 + xy + y = x^3 + x^2 + 22x - 9$ sobre $\mathbb{Q}_5$ (LMFDB 50.b4). Como $\Delta = -819200 = 2 \cdot 5^2 + \dots$ e $c_4 = -1055 = 1 \cdot 5 + \dots$, E tem redução aditiva módulo v_5 .

Exemplo 2.2.9. A curva elíptica $E: y^2 = x^3 - 9x$ sobre $\mathbb{Q}$ (LMFDB 288.d3) tem discriminante $\Delta = 46656 = 2^6 \cdot 3^6$ e $c_4 = 432 = 2^4 \cdot 3^3$. A redução de E é instável, sendo

- Aditiva em $p = 2$ e 3 ;
- Boa em $p \geq 5$.

Considere a mesma curva elíptica sobre $\mathbb{Q}(\mu_6)$, onde $\mu_6 \doteq e^{2\pi i/6}$ (note que $3 = \mu_6^5(1 + \mu_6)^2$ não é primo em $\mathbb{Z}[\mu_6]$!). A mudança de coordenadas $(x, y) = ((\mu_6^2 + \mu_6)^2 x' + (\mu_6^2 + \mu_6)^3 y')$ coloca a equação na forma $y^2 = x^3 - x$ (LMFDB 1024.1-a1), cujo discriminante minimal global é $\mathfrak{D}_{\min}(E) = (64) = (2)^6$ e $c_4 = 48 = \mu_6^5 \cdot 2^4 \cdot (1 + \mu_6)^2$. A redução de E em $\mathfrak{p} = (1 + \mu_6)$, o primo sobre 3 , passa a ser boa^[92].

Conclusão: a redução de uma curva elíptica depende do corpo sobre o qual ela está definido, e que reduções más podem “melhorar” em extensões do corpo inicial^[93].

Encerramos esta seção com a definição de um importante número associado às curvas elípticas sobre $\mathbb{Q}$:

Definição 2.2.10. O **condutor** de $E/\mathbb{Q}$ é o inteiro positivo

$$N_E \doteq \prod_p p^{f_p}, \quad \text{onde } f_p = \begin{cases} 0, & \text{se } E \text{ tem boa redução módulo } p \\ 1, & \text{se } E \text{ tem redução multiplicativa módulo } p \\ 2, & \text{se } E \text{ tem redução aditiva módulo } p \notin \{2, 3\} \\ 2 + \delta_p, & \text{se } E \text{ tem redução aditiva módulo } p \in \{2, 3\}. \end{cases} \quad [94]$$

Note que este produto é finito, pois apenas finitos primos dividem $\Delta_{\min}(E)$. Posto de outra maneira, N_E “coleta” os primos em que E tem má redução.

2.3 Curvas elípticas sobre $\mathbb{C}$

Seja $K = \mathbb{C}$. Vamos verificar nesta subseção que *curvas elípticas complexas têm a forma de toros*. Por conveniência, as curvas elípticas complexas serão consideradas não numa das formas de Weierstrass apresentadas anteriormente, mas na forma

$$y^2 = 4x^3 - ax - b, \quad (2.5)$$

^[92]Nesse caso, dizemos que E tem redução **potencialmente boa** em 3 , isto é, a redução passa a ser boa sobre um primo correspondente em alguma extensão.

^[93]Note que um primo num certo corpo de números pode deixar de ser primo numa extensão finita, ou seja, a equação considerada pode deixar de ser um modelo minimal.

^[94]O inteiro δ_p é dado pela Fórmula de Ogg–Saito (SILVERMAN, 2009, p. 450, Proposição C.16.2).

imediatamente derivada da forma (2.3). O motivo para isto é que o discriminante e o j -invariante de uma curva elíptica nesta forma assumem as (familiares) aparências

$$\Delta = 16(a^3 - 27b^2) \quad \text{e} \quad j = 1728 \frac{a^3}{a^3 - 27b^2}.$$

Seja $\tau \in \mathbb{H}$. Como $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2 \neq 0$,

$$E_\tau: y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

é uma curva elíptica, que diremos **normalizada**, e $j(E_\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} = j(\tau)$.

Portanto, dada uma curva elíptica E , pela sobrejetividade de j , $j(E) = j(\tau)$ para algum $\tau \in \mathbb{H}$, donde $E \cong E_\tau$. Logo, toda curva elíptica é isomorfa a uma curva elíptica normalizada.

2.3.1 Toros complexos

Definição 2.3.1. Sejam $\omega_1, \omega_2 \in \mathbb{C}$ linearmente independentes sobre $\mathbb{R}$. O **reticulado** gerado por ω_1 e ω_2 é o subgrupo discreto $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. O quociente do plano complexo por este reticulado dá origem ao **toro complexo** $\mathbb{C}/\Lambda$.

Figura 4 – Como ver $\mathbb{C}/\Lambda$ como um toro

Fonte: Elaborada pelo autor.

Em geral, pediremos também que $\omega_1/\omega_2 \in \mathbb{H}$. Esta condição faz com que a matrizes de mudança de base sejam elementos de $\text{SL}_2(\mathbb{Z})$:

$$\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \mathbb{Z}\omega'_1 \oplus \mathbb{Z}\omega'_2 \iff \begin{bmatrix} \omega'_1 \\ \omega'_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} \quad \text{para algum} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z}).$$

Toros são ao mesmo tempo grupos abelianos com a soma herdada de $\mathbb{C}$ e Superfícies de Riemann (veja [Miranda \(1995\)](#)). Uma **isogenia** é um mapa entre toros que leva em conta estas duas estruturas: é simultaneamente um morfismo de grupos e uma função holomorfa. Uma isogenia invertível por outro isogenia é um **isomorfismo**.

Proposição 2.3.2. Se $f: \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda'$ é uma isogenia, existe $\alpha \in \mathbb{C}^\times$ tal que $f(z + \Lambda) = \alpha z + \Lambda'$ (em particular, $\alpha\Lambda \subseteq \Lambda'$). Além disso, f é um isomorfismo $\iff \alpha\Lambda = \Lambda'$ ([DIAMOND; SHURMAN, 2005](#), p. 26, Proposição 1.3.2).

Em particular, como $\frac{1}{\omega_2}(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) = \mathbb{Z}\frac{\omega_1}{\omega_2} \oplus \mathbb{Z}$, todo toro é isomorfo a um **toro normalizado** $\mathbb{C}/\Lambda_\tau$, onde $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$, com $\tau \in \mathbb{H}$. Além disso,

$$\mathbb{C}/\Lambda_{\tau_1} \cong \mathbb{C}/\Lambda_{\tau_2} \iff \mathrm{SL}_2(\mathbb{Z}) \cdot \tau_1 = \mathrm{SL}_2(\mathbb{Z}) \cdot \tau_2.$$

2.3.2 Curvas elípticas complexas são toros

Vamos supor, sem perda de generalidade, que todos os toros e curvas elípticas até o fim desta seção são normalizados.

Definição 2.3.3. Seja $\tau \in \mathbb{H}$. Definimos a **função $\wp_\tau$ de Weierstrass** por

$$\wp_\tau(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda_\tau - \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right), \quad z \in \mathbb{C} - \Lambda_\tau.$$

Cada termo da soma acima é da ordem de $\frac{z}{\omega^3}$, o que assegura a convergência absoluta da série (WASHINGTON, 2008, p. 262, Teorema 9.3).

É fácil ver que $\wp_\tau(z)$ é par. Apesar de não ser inicialmente claro, esta função é Λ_τ -periódica (i.e. $\wp_\tau(z + \lambda) = \wp_\tau(z)$, $\forall \lambda \in \Lambda_\tau$): Sua derivada

$$\wp'_\tau(z) = -2 \sum_{\omega \in \Lambda_\tau} \frac{1}{(z - \omega)^3}$$

é claramente Λ_τ -periódica, além de ser ímpar, isto é, $\wp'_\tau(-z) = -\wp'_\tau(z)$. Disto, se $\lambda \in \Lambda_\tau$,

$$(\wp_\tau(z + \lambda) - \wp_\tau(z))' = \wp'_\tau(z + \lambda) - \wp'_\tau(z) = 0 \implies \wp_\tau(z + \lambda) - \wp_\tau(z) = k.$$

Fazendo $z = -\lambda/2$, obtemos que $k = 0$ e $\wp_\tau$ é Λ_τ -periódica.

Perto de 0, obtemos as seguintes expansões para $\wp_\tau$ e $\wp'_\tau$:

$$\wp_\tau(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n \text{ par}}}^{\infty} G_{n+2}(\tau)(n+1)z^n \quad \text{e} \quad \wp'_\tau(z) = -\frac{2}{z^3} + \sum_{\substack{n=2 \\ n \text{ par}}}^{\infty} G_{n+2}(\tau)n(n+1)z^{n-1}.$$

Comparando os primeiros termos dos desenvolvimentos das séries acima, vemos que a função $f(z) = \wp'_\tau(z)^2 - 4\wp_\tau(z)^3 + 60G_4(\tau)\wp_\tau(z) + 140G_6(\tau)$ é da ordem de z^2 , Λ_τ periódica e limitada. Logo, pelo Teorema de Liouville (AHLFORS, 1979, p. 122),

$$\wp'_\tau(z)^2 = 4\wp_\tau(z)^3 - \underbrace{60G_4(\tau)}_{=g_2(\tau)}\wp_\tau(z) - \underbrace{140G_6(\tau)}_{=g_3(\tau)},$$

ou seja, $(\wp_\tau(z), \wp'_\tau(z)) \in E_\tau$.

Teorema 2.3.4 (Uniformização). Um toro e sua correspondente curva elíptica são isomorfos como grupos abelianos:

$$\varphi: \mathbb{C}/\Lambda_\tau \xrightarrow{\sim} E_\tau(\mathbb{C}), \quad z + \Lambda_\tau \mapsto \begin{cases} (\wp_\tau(z), \wp'_\tau(z)) & z \notin \Lambda_\tau \\ O & z \in \Lambda_\tau. \end{cases}$$

Prova. Assumiremos alguns fatos elementares sobre funções Λ -periódicas (WASHINGTON, 2008, p. 259, Teorema 9.1): se f é uma destas funções e Π é o paralelogramo fundamental de Λ (isto é, um domínio fundamental do quociente $\mathbb{C}/\Lambda$),

$$\int_{\partial\Pi} \frac{f'(z)}{f(z)} dz = 0 \implies \sum_{p \in \Pi} v_p(f) = 0; \quad (2.6)$$

$$\int_{\partial\Pi} z \frac{f'(z)}{f(z)} dz = 0 \implies \sum_{p \in \Pi} v_p(f)p \equiv 0 \pmod{\Lambda}. \quad (2.7)$$

Tome $z_0 \in \Pi - \{0\}$ ^[95]. A função $f(z) = \wp_\tau(z) - \wp_\tau(z_0)$ é Λ_τ -periódica com apenas um polo duplo em 0 e um zero z_0 . Logo, por (2.6), f possui um outro zero em Π que, pela paridade de $\wp_\tau$, é $-z_0$. Da mesma forma, $g(z) = \wp'_\tau(z) - \wp'_\tau(z_0)$ possui apenas um polo triplo em 0 e um zero em z_0 . Porém, como z_0 é zero simples de $\wp_\Lambda$, g não possui um zero em $-z_0$. Assim, z_0 é o único ponto que anula f e g simultaneamente. Logo, $\wp$ é injetora.

Tome $(a, b) \in E$. Temos que $\wp_\tau - a$ e $\wp'_\tau - b$ possuem polos em 0, donde, pelo comentário acima, também possuem zeros em Π . Portanto, $\wp$ é sobrejetora.

Sejam $P_1 = (\wp_\tau(z_1), \wp'_\tau(z_1))$ e $P_2 = (\wp_\tau(z_2), \wp'_\tau(z_2))$ pontos em E_τ , determinando uma reta $ax + by + c = 0$. Se $b \neq 0$, $f = a\wp_\tau + b\wp'_\tau + c$ possui apenas um polo triplo em 0 e, portanto, três zeros. Dois deles são z_1 e z_2 , possivelmente iguais. Seja z_3 o outro, que corresponde ao terceiro ponto na intersecção da reta com E_τ . Por (2.7),

$$-3 \cdot 0 + 1 \cdot z_1 + 1 \cdot z_2 + 1 \cdot z_3 \equiv 0 \pmod{\Lambda_\tau} \iff z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda_\tau}.$$

Assim, $\wp(z_1 + z_2 + \Lambda_\tau) = \wp(-z_3 + \Lambda_\tau) = -P_3 = P_1 + P_2 = \wp(z_1 + \Lambda_\tau) + \wp(z_2 + \Lambda_\tau)$.

Para o caso $b = 0$ (em que a reta é vertical), é basta fazer $P_3 = O$. ■

2.4 Curvas elípticas sobre $\mathbb{Q}_p$

Curiosamente, o caso p -ádico é muito parecido com o caso complexo: *curvas elípticas p -ádicas têm a forma de “toros p -ádicos”!* A seguir, deduziremos o comportamento das curvas elípticas p -ádicas fazendo paralelos com o caso complexo que acabamos de discutir.

Seja $\tau \in \mathbb{H}$ e considere a curva elíptica complexa normalizada

$$E_\tau: y^2 = 4x^3 - g_2(\tau)x - g_3(\tau).$$

Aplicando a mudança de variáveis $(x, y) \mapsto (x', y')$ dada por

$$\frac{1}{(2\pi i)^2}x = x' + \frac{1}{12} \quad \text{e} \quad \frac{1}{(2\pi i)^3}y = 2y' + x',$$

^[95]Por simplicidade, vamos supor que Π é um paralelogramo centrado em 0

podemos escrevê-la na forma $E_q: y^2 + xy = x^3 + a_4x + a_6$, com^[96]

$$a_4 = -\frac{1}{4(2\pi i)^4} g_2(\tau) + \frac{1}{48} = -5 \sum_{n=1}^{\infty} \sigma_3(n) q^n$$

$$a_6 = -\frac{1}{4(2\pi i)^6} g_3(\tau) - \frac{1}{48(2\pi i)^4} g_2(\tau) + \frac{1}{1728} = -\frac{1}{12} \sum_{n=1}^{\infty} (5\sigma_3(n) + 7\sigma_5(n)) q^n,$$

onde $\sigma_k(n) = \sum_{d|n} d^k$ e $q = e^{2\pi i \tau}$ (note que $|q| < 1$). Pela mudança de coordenadas acima:

$$\Delta(E_q) = \frac{\Delta(\tau)}{(2\pi i)^{12}} = \sum_{n=1}^{\infty} \tau(n) q^n \quad \text{e} \quad j(E_q) = j(\tau) = \frac{1}{q} + \sum_{n=1}^{\infty} c_n q^n.$$

Agora, pelo lado p -ádico: seja $q \in \mathbb{Q}_p$ com $|q|_p < 1$. Como acima, as séries

$$a_4(q) \doteq -5 \sum_{n=1}^{\infty} \sigma_3(n) q^n \quad \text{e} \quad a_6(q) \doteq -\frac{1}{12} \sum_{n=1}^{\infty} (5\sigma_3(n) + 7\sigma_5(n)) q^n$$

convergem p -adicamente. A cúbica p -ádica

$$E_q: y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

continua tendo discriminante não-nulo (dado pela mesma série de antes), donde é uma curva elíptica, que chamaremos **normalizada**, visto que E_q é a contraparte p -ádica da curva elíptica complexa normalizada E_τ . Observe que

$$|j(E_q)|_p = \left| \frac{1}{q} + \sum_{n=1}^{\infty} c_n q^n \right|_p = \frac{1}{|q|_p} \left| 1 + \sum_{n=1}^{\infty} c_n q^{n+1} \right|_p = \frac{1}{|q|_p} > 1.$$

No caso complexo, toda curva elíptica é isomorfa a uma normalizada: a ideia era usar a sobrejetividade da função modular j para encontrar $\tau \in \mathbb{H}$ com $j(E) = j(\tau) = j(E_\tau)$ e concluir que $E \cong E_\tau$. Aqui, algumas curvas elípticas p -ádicas com $|j(E)|_p > 1$ é que serão isomorfas a uma normalizada, e um fenômeno similar acontece:

Proposição 2.4.1. Dado $\alpha \in \overline{\mathbb{Q}}_p$ com $|\alpha|_p > 1$, existe um único $q \in \overline{\mathbb{Q}}_p^\times$ com $|q|_p < 1$ tal que $j(E_q) = \alpha$.

Prova. A recíproca da série $j(q) \in \mathbb{Z}[[q]]$ é dada por^[97]:

$$f(q) \doteq \frac{1}{j(q)} = \frac{q}{1 + \sum_{n=0}^{\infty} c_n q^{n+1}} = q + \cdots \in \mathbb{Z}[[q]].$$

^[96]Recorde as expansões de Fourier das séries de Eisenstein do Exemplo 1.7.5.

^[97]Se $S(t) = 1 + \sum_{n=1}^{\infty} c_n t^n$ possui coeficientes inteiros, sua recíproca S^{-1} também terá.

Assim, existe uma série formal $g \in \mathbb{Z}[[q]]$ tal que $g(f(q)) = q$. Como g também é da forma $g(q) = q + \dots$, para $|\lambda|_p < 1$, $|g(\lambda)|_p = |\lambda|_p$. Logo, temos que $\left|g\left(\frac{1}{\alpha}\right)\right|_p = \frac{1}{|\alpha|_p} < 1$. Tomando $q = g\left(\frac{1}{\alpha}\right)$, obtemos que

$$j(E_q) = j(q) = \frac{1}{f\left(g\left(\frac{1}{\alpha}\right)\right)} = \alpha.$$

Para a unicidade, suponha $\tilde{q}$ nas condições do enunciado. Temos que $f(q) = f(\tilde{q})$, donde

$$0 = |f(q) - f(\tilde{q})|_p = |q - \tilde{q}|_p \cdot \frac{1}{1 + \dots + \frac{1}{p}} = |q - \tilde{q}|_p \implies q = \tilde{q}. \quad \blacksquare$$

Porém, $\mathbb{Q}_p$ não é algebricamente fechado. Logo, a Proposição 2.1.14 apenas nos garante que, para cada curva elíptica E com $|j(E)|_p > 1$, existe uma (única^[98]) curva elíptica normalizada E_q tal que $E \cong E_q$ sobre $\overline{\mathbb{Q}_p}$. Para (possivelmente) descer para $\mathbb{Q}_p$, precisamos de um outro invariante.

Seja K uma extensão algébrica de $\mathbb{Q}_p$ e E uma curva elíptica com $j(E) \notin \{0, 1728\}$. Defina^[99]

$$\gamma_K(E) \doteq -\frac{2a}{b},$$

onde $E: y^2 = 4x^3 - ax - b$. É claro que a definição acima depende do corpo K sobre o qual a curva está definido, mas também da equação que define E . Porém, $\gamma_K(E)$ fica bem definido a menos de quadrados (Proposição 2.1.12). Portanto, apesar deste detalhe, faz sentido considerar a extensão quadrática $L = K(\sqrt{\gamma_K(E)})$.

Lema 2.4.2. Se $\alpha \in K$ é tal que $|\alpha|_p < 1$, $4\alpha + 1 \in (K^\times)^2$.

Prova. Com α nas condições do enunciado, a série

$$(4\alpha + 1)^{-1/2} = \sum_{n=0}^{\infty} \binom{-1/2}{n} (4\alpha)^n = \sum_{n=0}^{\infty} (-1)^n \binom{2n}{n} \alpha^n \in \mathbb{Z}[[\alpha]]$$

converge. Logo, $(4\alpha + 1)^{-1}$, e portanto $4\alpha + 1$, é um quadrado em $K^\times$. ■

Proposição 2.4.3. Seja K um corpo p -ádico e duas curvas elípticas E_1 e E_2 sobre K . Se $j(E_1) = j(E_2) \notin \{0, 1728\}$ e $\gamma_K(E_1) \equiv \gamma_K(E_2) \pmod{(K^\times)^2}$, então E_1 e E_2 são isomorfas sobre K .

Prova. Sejam $E_1: y^2 = 4x^3 - a_1x - b_1$ e $E_2: y^2 = 4x^3 - a_2x - b_2$. Então,

$$j(E_1) = j(E_2) \implies a_1^3 b_2^2 = a_2^3 b_1^2.$$

^[98]No caso $K = \mathbb{C}$, a unicidade era a menos da ação de $\mathrm{SL}_2(\mathbb{Z})$, i.e., $\mathrm{SL}_2(\mathbb{Z}) \cdot \tau_1 = \mathrm{SL}_2(\mathbb{Z}) \cdot \tau_2 \iff E_{\tau_1} \cong E_{\tau_2}$.

^[99]Na forma 2.3 $y^2 = x^3 - 27c_4x - 54c_6$, $\gamma_K(E) = -\frac{c_4}{c_6}$.

Segue da outra hipótese que

$$\gamma_K(E_1) \equiv \frac{2a_1}{b_1} \equiv \frac{2a_2}{b_2} \equiv \gamma_K(E_2) \pmod{(K^\times)^2} \implies a_1 b_2 = t^2 a_2 b_1,$$

com $t \in K^\times$. Logo, o mapa $E_1 \rightarrow E_2$ dado por $(x, y) \mapsto (t^2 x, t^3 y)$ é um isomorfismo sobre K . ■

Para uma curva elíptica normalizada E_q , calcula-se que

$$\gamma_K(E_q) = \frac{1 - 48a_4(q)}{1 - 72a_4(q) + 864a_6(q)} = \frac{1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n}{1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n} \in (K^\times)^2.$$

Logo, temos um critério para saber quando uma curva elíptica E com $|j(E)|_p > 1$ ^[100] e a correspondente curva normalizada $E_q \cong E$ são isomorfas também sobre $\mathbb{Q}_p$:

$$E_q \cong E \text{ sobre } \mathbb{Q}_p \iff \gamma_{\mathbb{Q}_p}(E) \in (\mathbb{Q}_p^\times)^2.$$

Infelizmente, isto nem sempre é garantido. Porém, na pior das hipóteses, sempre podemos conseguir um isomorfismo entre E e E_q sobre a extensão quadrática $K = \mathbb{Q}_p(\sqrt{\gamma_{\mathbb{Q}_p}(E)})$.

2.4.1 Curva de Tate

Um toro complexo fica bem determinado por um reticulado (um subgrupo discreto não-trivial de $\mathbb{C}$). Porém, nos números p -ádicos, subgrupos assim não existem:

Proposição 2.4.4. Todo subgrupo $\Lambda \subseteq \mathbb{Q}_p$ se acumula em 0.

Prova. Basta tomar $t \neq 0$ em Λ e notar que os termos da sequência $(p^n t)_n \subseteq \Lambda$ são divisíveis por potências cada vez maiores de p , donde converge para 0. ■

Logo, tentemos enxergar os toros de outra maneira: pela aplicação do mapa exponencial $z \mapsto u = e^{2\pi iz}$, o toro $\mathbb{C}/\Lambda_\tau$ é expresso como $\mathbb{C}^\times/q^\mathbb{Z}$, onde $q^\mathbb{Z} = \{e^{2\pi i n \tau}, n \in \mathbb{Z}\}$. Analogamente, tomando $q \in \mathbb{Q}_p^\times$ com $|q|_p < 1$, consideramos o quociente $\mathbb{Q}_p^\times/q^\mathbb{Z}$, onde $q^\mathbb{Z} = \{q^n, n \in \mathbb{Z}\}$, que chamamos de **curva de Tate** (“toro p -ádico”).

Assim como usamos q como a contraparte p -ádica de $q = e^{2\pi i \tau}$, vamos usar a variável u como a contraparte p -ádica de $u = e^{2\pi iz}$, a variável z usual na forma exponencial.

^[100]Em particular, $j(E) \notin \{0, 1728\}$.

2.4.2 Curvas elípticas p -ádicas são “toros”

No caso complexo, o isomorfismo entre uma curva elíptica normalizada e um toro era dado pela função $\wp_\tau$ de Weierstrass e sua derivada. Mudando para a notação exponencial, estas funções podem ser escritas como (onde $q = e^{2\pi i\tau}$ e $u = e^{2\pi iz}$)

$$\frac{1}{(2\pi i)^2} \wp_\tau(z) - \frac{1}{12} = \sum_{n=-\infty}^{\infty} \frac{q^n u}{(1 - q^n u)^2} - 2 \sum_{n=1}^{\infty} \frac{q^n}{(1 - q^n)^2},$$

$$\frac{1}{(2\pi i)^3} \wp'_\tau(z) = \sum_{n=-\infty}^{\infty} \frac{(q^n u)^2}{(1 - q^n u)^3} + \sum_{n=1}^{\infty} \frac{q^n}{(1 - q^n)^2}.$$

Aplicando a mudança de coordenadas anterior, obtemos as séries

$$X_q(u) = \sum_{n=-\infty}^{\infty} \frac{q^n u}{(1 - q^n u)^2} - 2 \sum_{n=1}^{\infty} \frac{q^n}{(1 - q^n)^2} \quad \text{e} \quad Y_q(u) = \sum_{n=-\infty}^{\infty} \frac{(q^n u)^2}{(1 - q^n u)^3} + \sum_{n=1}^{\infty} \frac{q^n}{(1 - q^n)^2}.$$

Nestas condições, o teorema da uniformização complexo se torna

$$\varphi: \mathbb{C}^\times / q^\mathbb{Z} \xrightarrow{\sim} E_q(\mathbb{C}), \quad u \mapsto \begin{cases} (X_q(u), Y_q(u)) & , \text{ se } u \notin q^\mathbb{Z} \\ O & , \text{ se } u \in q^\mathbb{Z}. \end{cases}$$

Novamente, o caso p -ádico imita o caso complexo:

Teorema 2.4.5 (Uniformização p -ádica). Seja $q \in \mathbb{Q}_p^\times$ tal que $|q|_p < 1$. Então, a curva de Tate $\mathbb{Q}_p^\times / q^\mathbb{Z}$ e a curva elíptica normalizada $E_q(\mathbb{Q}_p)$ são isomorfas como grupos abelianos.

Ideias da Prova. [101] Definimos as séries p -ádicas $X_q(u)$ e $Y_q(u)$ exatamente como acima. É fácil checar que estas séries convergem e que são q -periódicas, isto é,

$$X_q(qu) = X_q(u) \quad \text{e} \quad Y_q(qu) = Y_q(u).$$

Mostra-se que o **mapa de Tate**

$$\Phi_q: \overline{\mathbb{Q}_p}^\times \rightarrow E_q(\overline{\mathbb{Q}_p}), \quad u \mapsto \begin{cases} (X_q(u), Y_q(u)) & , \text{ se } u \notin q^\mathbb{Z} \\ O & , \text{ se } u \in q^\mathbb{Z} \end{cases}$$

é um morfismo de grupos (usando identidades de séries formais obtidas a partir das fórmulas para a soma de dois pontos em uma curva elíptica - trabalhoso, mas fácil) sobrejetor (esta é a parte difícil!) com núcleo $q^\mathbb{Z}$ (imediato). Logo, temos um isomorfismo $\overline{\mathbb{Q}_p}^\times / q^\mathbb{Z} \cong E_q(\overline{\mathbb{Q}_p})$. Para concluir a prova, basta notar que Φ_q comuta com a ação de $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. $\square$

[101] Diferentemente do caso complexo, porém, a prova deste teorema é bastante trabalhosa. O esboço a seguir segue aproximadamente a prova detalhada apresentada no livro de Silverman (1994, Seções V.3 e V.4).

2.4.3 Invariante de Mazur–Tate–Teitelbaum

Vimos anteriormente que toda curva elíptica p -ádica E com $|j(E)|_p > 1$ é isomorfa (sobre $\overline{\mathbb{Q}_p}$) a uma única curva normalizada E_q , onde $q \in \mathbb{Q}_p$ é tal que $|q|_p < 1$. A este q chamamos **período de Tate de E sobre p** . Vimos também que nem sempre o isomorfismo acima está definido sobre $\mathbb{Q}_p$, e um critério para quando isto ocorre. Porém, um certo tipo de curva elíptica sempre satisfaz este critério:

Proposição 2.4.6. Seja $E/\mathbb{Q}_p$ uma curva elíptica com redução multiplicativa *split* de período de Tate q sobre p . Então, $E \cong E_q$ sobre $\mathbb{Q}_p$.

Prova. Primeiramente, note que, como E tem redução multiplicativa em p , $|\Delta(E)|_p < 1$ e $|c_4|_p = 1$, donde $|j(E)|_p > 1$.

Pela Proposição 2.4.3, basta mostrarmos que $\gamma_{\mathbb{Q}_p}(E) \in (\mathbb{Q}_p^\times)^2$. Seja

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

um modelo p -integral de E . Por uma translação, podemos supor que a singularidade de $\tilde{E}$ é $(\bar{0}, \bar{0})$, ou seja, $a_3 \equiv a_4 \equiv a_6 \equiv 0 \pmod{v_p}$. Disto, $b_4 \equiv b_6 \equiv 0 \pmod{v_p}$ e $b_2 \equiv a_1^2 \pmod{v_p}$. Como E tem redução multiplicativa, $c_4 = b^2 - 24b_4 \equiv b_2^2 \not\equiv 0 \pmod{v_p}$. Logo, $b_2 \in \mathbb{Z}_p^\times$.

Calculemos $\gamma_{\mathbb{Q}_p}(E)$. Pela nota [99],

$$\gamma_{\mathbb{Q}_p}(E) = -\frac{c_4}{c_6} = -\frac{b_2^2 - 24b_4}{-b_2^3 + 36b_2b_4 - 216b_6} \equiv \frac{1}{b_2} \cdot \frac{1 - 4 \cdot \left(6 \cdot \frac{b_4}{b_2^2}\right)}{1 - 4 \cdot \left(9 \cdot \frac{b_4}{b_2^2} - 54 \cdot \frac{b_6}{b_2^3}\right)} \pmod{(\mathbb{Q}_p^\times)^2}.$$

Note que os termos entre parênteses são congruentes a 0 módulo p . Logo, pelo Lema 2.4.2, $\gamma_{\mathbb{Q}_p}(E) \equiv \frac{1}{b_2^2} \pmod{(\mathbb{Q}_p^\times)^2}$.

Fatore $\tilde{E}: x^3 = y^2 + \bar{a}_1xy - \bar{a}_2x^2 = (y - \bar{\alpha}x)(y - \bar{\beta}x)$. Como E tem redução multiplicativa *split* em p , $\bar{\alpha}, \bar{\beta} \in \mathbb{F}_p$ e $\bar{\alpha} \neq \bar{\beta}$. Fazendo $x = 1$, $\bar{\alpha}$ e $\bar{\beta}$ são raízes do polinômio $\bar{f}(y) = y^2 + \bar{a}_1y - \bar{a}_2$. Pelo Lema de Hensel (Teorema 1.4.15), $\bar{\alpha}$ e $\bar{\beta}$ se levantam para $\alpha, \beta \in \mathbb{Z}_p$, respectivamente, raízes de $f(y) = y^2 + a_1y - a_2$. Logo, $y^2 + a_1yx - a_2x^2 = (y - \alpha x)(y - \beta x) \implies b_2 = a_1^2 + 4a_2 = (\alpha - \beta)^2 \in (\mathbb{Q}_p^\times)^2$. Portanto, $\gamma_{\mathbb{Q}_p}(E) \equiv 1 \pmod{(\mathbb{Q}_p^\times)^2}$. ■

Definição 2.4.7. Seja E nas condições da Proposição 2.4.6. Definimos o **invariante de Mazur–Tate–Teitelbaum** de E por

$$\mathcal{L}_p(E) = \frac{\log_p(q)}{v_p(q)} \in \mathbb{Z}_p,$$

onde $\log_p: \mathbb{Q}_p^\times \rightarrow p\mathbb{Z}_p$ é o logaritmo p -ádico (ver seção 1.5.2).

Exemplo 2.4.8. A curva elíptica $E: y^2 + xy + y = x^3 + x + 2$ sobre $\mathbb{Q}$ do Exemplo 2.2.4 possui redução multiplicativa *split* em $p = 3$ e $|j(E)|_3 = \left| \frac{103823}{1413} \right|_3 = 9 > 1$. O *software* PARI/GP^[102] nos dá que $\mathcal{L}_3(E) = 1$.

Observação 2.4.9. O invariante que acabamos de definir satisfaz a seguinte relação, conjecturada por Mazur, Tate e Teitelbaum (1986) e provada por Greenberg e Stevens (1993), no contexto dos análogos p -ádicos da conjectura BSD:

$$L'_p(E, 1) = \mathcal{L}_p(E) \frac{L(E, 1)}{\Omega_E},$$

onde L_p é a L -função p -ádica de Mazur–Swinnerton-Dyer (BERTOLINI; DARMON, 2007, p. 13), L é a L -função de Hasse–Weil (Definição 3.2.2) e Ω_E é o período real de E (ver seção A.1.3).

^[102]Código:

```
E = ellinit([1 + 0(3), 1 + 0(3), 1 + 0(3), 1 + 0(3), 2 + 0(3)]);
E.tate
```

O comando `tate` nos dá diversas informações sobre o modelo p -ádico de E , como o próprio período de Tate, além do invariante de Mazur-Tate-Teitelbaum que acabamos de discutir. Veja o guia do usuário do PARI/GP (The PARI Group, 2018b, p. 424)

CURVAS ELÍPTICAS SOBRE $\mathbb{Q}$

Quantos pontos $\mathbb{Q}$ -racionais uma curva plana não-singular não-vazia sobre $\mathbb{Q}$ possui?

- Se $g(C) = 0$, existe um mapa birracional $\mathbb{P}^1(\mathbb{Q}) \dashrightarrow C(\mathbb{Q})$. Logo, C tem *infinitos* pontos.
- Se $g(C) \geq 2$, C possui *finitos* pontos, por um resultado não-trivial de [Faltings \(1983\)](#).

Quanto ao caso intermediário $g(C) = 1$, que é justamente o das curvas elípticas, C pode ter finitos ou infinitos pontos: a curva $C_k: y^2 = x^3 + k$ possui ([CONRAD, 2019c](#), p. 10)

- 1 ponto $\mathbb{Q}$ -racional, para $k = -1$;
- 2 pontos $\mathbb{Q}$ -racionais, para $k = 16$;
- 5 pontos $\mathbb{Q}$ -racionais, para $k = 1$;
- infinitos pontos $\mathbb{Q}$ -racionais, para $k = -2$.

O comportamento “anômalo” deste caso levanta ainda mais perguntas: dada uma curva elíptica E , é possível saber se ela tem finitos ou infinitos pontos racionais? Além disso, quantas curvas elípticas têm finitos e infinitos pontos, proporcionalmente?

3.1 O Teorema de Mordell–Weil e o posto algébrico

Seja E uma curva elíptica sobre $\mathbb{Q}$ ^[103]. O Teorema de Mordell–Weil afirma que o grupo $E(\mathbb{Q})$ é finitamente gerado:

^[103]Salvo menção em contrário, neste capítulo E sempre denota uma curva elíptica sobre $\mathbb{Q}$.

Teorema 3.1.1 (Mordell–Weil). Seja E uma curva elíptica sobre $\mathbb{Q}$. Então,

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}},$$

onde $E(\mathbb{Q})_{\text{tor}}$ é um grupo finito e $r \in \mathbb{Z}_{\geq 0}$.

Naturalmente, este teorema, cuja prova *não* é construtiva, levantou a seguinte pergunta: dados um grupo finito T e um inteiro não-negativo r , existe uma curva elíptica E sobre $\mathbb{Q}$ cujo grupo de pontos $\mathbb{Q}$ -racionais é $\mathbb{Z}^r \oplus T$? Uma conjectura de Ogg, provada por Mazur (1978), determina quais são as possibilidades para a parte de torção:

Teorema 3.1.2 (Mazur). Seja E uma curva elíptica sobre $\mathbb{Q}$. Então, $E(\mathbb{Q})_{\text{tor}}$ é um dos seguintes 15 grupos^[104]:

- $\mathbb{Z}/N\mathbb{Z}$, para $1 \leq N \leq 10$ ou $N = 12$;
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, para $1 \leq N \leq 4$.^[105]

O inteiro r do teorema de Mordell–Weil é chamado **posto algébrico** de E , denotado por $r_{\text{alg}}(E)$. Diferentemente da parte de torção, pouco se sabe sobre ele: não se sabe se $r_{\text{alg}}(E)$ pode ser qualquer inteiro não-negativo, muito menos se pode ser arbitrariamente grande^[106]. Os maiores exemplos conhecidos, ambos obtidos por Noam Elkies, não passam de 30!^[107] A curva elíptica com o maior posto determinado (obtida em 2009) é dada pela equação

$$y^2 + xy + y = x^3 - x^2 + 31368015812338065133318565292206590792820353345x + 302038802698566087335643188429543498624522041683874493555186062568159847,$$

e seu posto é 19. A curva elíptica de equação

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 \\ - 20067762415575526585033208209338542750930230312178956502x + \\ 34481611795030556467032985690390720374855 \\ 944359319180361266008296291939448732243429, \end{aligned}$$

^[104]Vale mencionar que todos os casos ocorrem infinitas vezes, isto é, para cada caso, existem infinitas curvas elípticas com j -invariantes distintos com tal grupo de torção (KUBERT, 1979).

^[105]A prova deste teorema é longa e intrincada. Para uma versão um pouco mais digesta, recomendamos ao leitor o curso em 23 aulas de Snowden (2013), lecionado na Universidade de Michigan e disponível em vídeo em sua página web.

^[106]A existência de curvas elípticas de posto algébrico arbitrariamente grande é uma conjectura “folclórica” da área. Porém, uma heurística recente de Park et al. (2018) desafia esta conjectura, sugerindo que apenas *finitas* curvas elípticas satisfazem $r_{\text{alg}}(E) > 21$!

^[107]Veja a página web de Dujella (2009) para um histórico dos postos algébricos recorde, bem como os maiores postos algébricos conhecidos para cada tipo de grupo de torção possível.

obtida em 2006, possui posto algébrico ≥ 28 , isto é, foram encontrados 28 pontos de ordem infinita independentes, mas, *a priori*, poderia haver mais!^[108]

Esta incerteza em até mesmo determinar o posto algébrico de uma curva elíptica concreta mostra quão difícil é o problema com que estamos lidando. Claro que, na prática, os cálculos são confiados aos computadores, mas, mesmo com o auxílio de um computador, calcular o posto algébrico de uma curva elíptica permanece uma tarefa não-trivial: não se conhece nenhum método que seja garantido funcionar para qualquer curva elíptica!^[109]

A dificuldade em se calcular o posto algébrico, além de frustrar nossas tentativas de desvendar a natureza das curvas elípticas sobre $\mathbb{Q}$, reside no coração de diversos problemas em aberto. No entanto, a Conjectura BSD propõe uma maneira simples de determiná-lo.

Observação 3.1.3. Recorde a pergunta posta no começo do capítulo. Pela discussão acima, uma curva elíptica tem infinitos pontos se, e somente se, $r_{\text{alg}}(E) > 0$. Logo, saber se uma curva elíptica tem finitos ou infinitos pontos é, em geral, uma pergunta difícil de responder.

3.1.1 Observações sobre a prova do Teorema de Mordell–Weil

A prova do Teorema de Mordell–Weil (3.1.1) consiste de duas partes: prova-se uma versão fraca do teorema e, deste, obtém-se a versão forte por um argumento mais geral chamado **descida infinita**, que envolve o uso de funções de altura.

Definição 3.1.4. Seja G um grupo abeliano. Uma função $h: G \rightarrow \mathbb{R}$ é uma **função de altura** se

1. Seja $Q \in G$. Existe uma constante $C_1(Q)$ tal que $h(P + Q) \leq 2h(P) + C_1(Q)$, para todo $P \in G$;
2. Existe $m \geq 2$ e C_2 (que só depende de G) tal que $h(mP) \geq m^2h(P) - C_2$, para todo $P \in G$;
3. Para toda constante C_3 , o conjunto $\{P \in G; h(P) \leq C_3\}$ é finito.

A condição (i) motiva o nome “altura”. A condição (ii) nos diz que multiplicações por inteiro tendem a aumentar a altura de um ponto, enquanto que (iii) determina que apenas finitos pontos estão abaixo de certa altura.

Observação 3.1.5. Considere os números 100 e $\frac{9999999}{100000}$. Seus valores são muito próximos, mas temos a impressão de que o segundo deles é, de certa forma, mais “complexo”. A altura mede, essencialmente, esse tipo de “complexidade”. Conforme [Silverman e Tate \(2015\)](#), p. 65, pode-se pensar na altura de um ponto como o número de *bits* necessários para armazená-lo num computador.

^[108]É mais provável que não haja: um artigo de [Klagsbrun, Sherman e Weigandt \(2016\)](#) mostra que, supondo-se a Hipótese de Riemann Generalizada (Conjectura 1.8.2), o posto algébrico desta curva elíptica é exatamente 28.

^[109]Veja a seção 3.3.1 para mais informações sobre os aspectos práticos da computação do grupo, e em particular do posto algébrico, de uma curva elíptica.

Teorema 3.1.6 (Descida infinita). Seja G um grupo abeliano. Suponha que exista uma função de altura $h: G \rightarrow \mathbb{R}$ e que G/mG é finito, onde m é o inteiro da condição (ii) da Definição 3.1.4. Então, G é finitamente gerado.

Prova. Sejam $Q_1, \dots, Q_r$ representantes das classes laterais de G/mG e tome $P \in G$. Defina $P_1 = \frac{1}{m}(P - Q_{i_1})$, para algum $1 \leq i_1 \leq r$, e, indutivamente,

$$P_j = \frac{1}{m}(P_{j-1} - Q_{i_j}) \quad \text{com } 1 \leq i_j \leq r,$$

para $1 \leq j \leq n$, que ainda não fixamos. Pelas propriedades (i) e (ii) de altura, temos que

$$h(P_j) \leq \frac{1}{m^2}(2h(P_{j-1}) + C'_1 + C_2)$$

(onde C'_1 é máximo das C_1 's obtidas por (i) para cada j). Iterando esta desigualdade, obtemos que (aqui usamos $m \geq 2$!)

$$h(P_n) \leq \frac{1}{2^n}h(P) + \frac{C'_1 + C_2}{2}.$$

Logo, para um n suficientemente grande, $h(P_n)$ é limitado por $1 + \frac{C'_1 + C_2}{2}$. Como

$$P = m^n P_n + \sum_{j=1}^n m^{j-1} Q_{i_j},$$

temos que $\{Q_1, \dots, Q_r\} \cup \left\{ Q \in G; h(Q) \leq 1 + \frac{C'_1 + C_2}{2} \right\}$, que é finito pela propriedade (iii) de altura, gera G . ■

Observação 3.1.7. A **descida infinita** é uma técnica indutiva pela qual se obtém, a partir de um objeto que satisfaz determinadas propriedades, uma sucessão infinita de objetos com as mesmas propriedades. Por exemplo, a partir de uma solução para uma equação diofantina, construímos infinitas soluções; ou, no nosso contexto atual, a partir de finitos elementos do grupo G , obtemos infinitos elementos, que é a ideia central do Teorema de Mordell-Weil^[110].

Agora, resta definirmos uma função de altura conveniente. Para $t = \frac{p}{q} \in \mathbb{Q}$ expresso na forma irredutível, seja $H(t) = \max\{|p|, |q|\}$.

Definição 3.1.8. Seja $E: y^2 = x^3 + ax + b$ uma curva elíptica sobre $\mathbb{Q}$. A função de **altura logarítmica** (ou *naïve*) $h_x: E(\mathbb{Q}) \rightarrow \mathbb{R}$ é definida por

$$h_x(P) = \begin{cases} \log H(x(P)), & \text{se } P \neq O \\ 0, & \text{se } P = O, \end{cases}$$

^[110]Historicamente, a descida infinita aparece frequentemente acompanhada do princípio da boa ordenação dos números naturais para fazer demonstrações por contradição: a ideia é usar a descida infinita para gerar uma sucessão infinita de soluções que implicaria a existência de uma sequência estritamente decrescente de números naturais, contradizendo o princípio da boa ordenação. Fermat, nome a que a descida infinita é frequentemente associada, a utilizou para provar que $x^4 + y^4 = z^2$ não admite soluções inteiras não-triviais (em particular, o caso $n = 4$ do Último Teorema de Fermat (MARTINEZ et al., 2013, p. 153, Exemplo 4.21)) e para mostrar que 1 não é um número congruente (veja subseção A.2.1).

onde $x(P)$ denota a abscissa^[111] de $P \in E(\mathbb{Q})$.

Proposição 3.1.9. A função h_x definida acima é uma função de altura, com $m = 2$ (SILVERMAN, 2009, p. 221, Lema VIII.4.1).

Logo, para provar o Teorema de Mordell–Weil, basta, pelo Teorema da Descida Infinita, mostrar que $E(\mathbb{Q})/2E(\mathbb{Q})$ é finito.

O Teorema de Mordell–Weil pode ser generalizado para curvas elípticas sobre um corpo de números $\mathbb{K}/\mathbb{Q}$, e a sua demonstração segue, *mutatis mutandis*^[112], o mesmo roteiro do caso particular que acabamos de discutir.

Teorema 3.1.10 (Mordell–Weil). Seja $E/\mathbb{K}$ uma curva elíptica. Então, $E(\mathbb{K})$ é finitamente gerado.

E, novamente, é necessário antes provar uma versão mais fraca do teorema:

Teorema 3.1.11 (Mordell–Weil, fraco). Seja E uma curva elíptica sobre $\mathbb{K}$. Então, para todo $m \geq 2$, $E(\mathbb{K})/mE(\mathbb{K})$ é finito^[113].

A demonstração do Teorema 3.1.11 será apresentada no capítulo seguinte.

3.2 *L-funções e o posto analítico*

Seja p primo e E uma curva elíptica. Quantos pontos há na redução módulo p de E ?

Temos $\frac{p-1}{2}$ quadrados não-nulos em $\mathbb{F}_p$ ^[114]. Assim, é esperado que $\tilde{E}(\mathbb{F}_p)$ tenha p pontos afins^[115]. Porém, isto nem sempre acontece:

Exemplo 3.2.1. A curva elíptica $E: y^2 = x^3 + x + 2$ do Exemplo 2.2.7 tem:

- 23 soluções módulo 17 (6 a mais do que o esperado);
- 11 soluções módulo 19 (8 a menos do que o esperado);
- 23 soluções módulo 23 (exatamente o esperado).

^[111]Note que, portanto, h_x depende da equação de Weierstrass escolhida para E .

^[112]A função de altura, por exemplo, precisa ser adaptada: veja (SILVERMAN, 2009, p. 234, Seção VIII.6) para uma discussão.

^[113]Para a prova do Teorema de Mordell–Weil só precisaríamos do caso $m = 2$, mas o caso geral também será útil.

^[114]Pois $(\mathbb{Z}/p\mathbb{Z})^\times$ é cíclico. Veja Conrad (2019b) para sete demonstrações distintas deste fato!

^[115]Isto é, se o polinômio cúbico em x na equação de Weierstrass de E “mistura bem” os valores de $x \in \mathbb{F}_p$, como é esperado de um polinômio, y^2 deve atingir uma vez cada um dos $\frac{p-1}{2}$ quadrados não-nulos, cada um originando 2 pontos, uma vez cada um dos $\frac{p-1}{2}$ não-quadrados, não contribuindo com nenhum ponto, e uma vez o 0, contribuindo com o ponto $(0,0)$. Ao todo, são $2 \cdot \frac{p-1}{2} + 0 \cdot \frac{p-1}{2} + 1 = p$ pontos. Outra maneira de pensar sobre isso é que “curvas são retas tortas” e a reta afim sobre $\mathbb{F}_p$ tem p pontos, então $\tilde{E}(\mathbb{F}_p)$ deveria ter também!

Coletamos a diferença entre as quantidades real e esperada de pontos de $\tilde{E}(\mathbb{F}_p)$ nos coeficientes^[116]

$$a_p(E) \doteq p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

Estendemos a definição dos coeficientes acima para todo índice natural fazendo

- (i) $a_1(E) \doteq 1$;
- (ii) $a_{p^e}(E) \doteq p^e + 1 - \#\tilde{E}(\mathbb{F}_{p^e})$, para todo $e > 1$;
- (iii) $a_{mn}(E) \doteq a_m(E)a_n(E)$ sempre que $\text{mdc}(m, n) = 1$.

Definição 3.2.2. A L -função (ou **função de Hasse–Weil**) de E é definida por

$$L(s, E) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}. \quad \text{Re}(s) > \frac{3}{2}, \text{ [117]}$$

Hasse e Weil, na década de 1960, conjecturaram que tal função tivesse extensão analítica e uma equação funcional relacionando um semiplano esquerdo com um semiplano direito do plano complexo, propriedades que já se sabia que as L -funções associadas a autoformas de Hecke possuíam.

Em 2001, um dos maiores problemas da história da Teoria dos Números é resolvido: a Conjectura de Taniyama–Shimura, que passou a se chamar Teorema da Modularidade, estabeleceu uma ponte entre o mundo das curvas elípticas e o das formas modulares, permitindo uma transferência de propriedades que eram conhecidas de um lado da ponte mas não do outro – em particular, as propriedades que tanto se desejavam que a função de Hasse–Weil satisfizesse.^[118]

Teorema 3.2.3 (Modularidade). Seja E uma curva elíptica sobre $\mathbb{Q}$. Então, existe uma autoforma $f_E \in \mathbb{S}_2(\Gamma_0(N_E))$ tal que $L(s, f_E) = L(s, E)$.

Com isto, podemos expressar a L -função de E como o produto de Euler

$$L(s, E) = \prod_{p \text{ primo}} \frac{1}{1 - a_p(E)p^{-s} + \mathbb{1}_E(p)p^{1-2s}},$$

onde $\mathbb{1}_E$ denota o caractere trivial módulo N_E , o condutor de E , isto é:

$$\mathbb{1}_E(p) = \begin{cases} 1, & \text{se } E \text{ tem redução boa em } p \\ 0, & \text{se } E \text{ tem redução má em } p. \end{cases}$$

^[116]Agora estamos considerando todos os pontos de $\tilde{E}(\mathbb{F}_p)$, ou seja, os pontos afins e o ponto no infinito O , por isto $p + 1$.

^[117]Isto segue da cota de Hasse–Weil (Teorema 1.1.5): $a_p(E) \leq 2\sqrt{p}$.

^[118]O teorema da Modularidade foi provado para curvas elípticas semi-estáveis por Wiles (1995) e Taylor e Wiles (1995), no âmbito da demonstração do Último Teorema de Fermat, e no caso geral por Breuil *et al.* (2001), adaptando a prova desse caso particular. Para uma introdução, referimos o leitor a Diamond e Shurman (2005) e, para mais detalhes a respeito da demonstração de Taylor–Wiles, recomendamos o livro de Cornell, Silverman e Stevens (1997), que consiste nas transcrições de um ciclo de palestras ocorrido em agosto de 1995 na Universidade de Boston acerca do então recém-provado Último Teorema de Fermat.

Em particular, $a_{p^e}(E)$ satisfaz a recorrência

$$a_{p^e}(E) = a_p(E)a_{p^{e-1}}(E) - \mathbb{1}_E(p)pa_{p^{e-2}}, \quad \forall e \geq 2. \quad (3.1)$$

Como a L -função da autoforma f_E pode ser estendida analiticamente para todo o plano complexo (Proposição 1.8.4), o mesmo vale para $L(s, E)$. Assim, faz sentido considerarmos a ordem de $L(s, E)$ em $s = 1$ ^[119], chamada **posto analítico** de E , e denotada por $r_{\text{an}}(E)$.

Observação 3.2.4. O ponto $s = 1$ é muito importante nos estudos das L -funções. Sem mencionar a própria conjectura de Birch e Swinnerton-Dyer, que apresentamos na próxima seção, o fato de $\zeta(s)$ ter um polo em $s = 1$ implica a existência de infinitos números primos, e o fato de uma L -função de Dirichlet $L(\chi, s)$ não possuir um zero em $s = 1$ implica que existem infinitos primos em progressão aritmética^[120].

Diferentemente do posto algébrico, o posto analítico pode ser calculado com relativa facilidade: existem algoritmos para calcular $L^{(r)}(1, E)$, logo o posto analítico de uma curva elíptica, com a precisão que se deseja (CREMONA, 1997, p. 42, seção 2.13)^[121].

3.2.1 Critérios para distinguir os tipos de redução boa

Nesta subseção, descrevemos dois critérios para distinguir se uma curva elíptica tem redução boa ordinária ou supersingular, baseado no coeficiente $a_p(E)$.

Proposição 3.2.5. Seja E uma curva elíptica e p um primo em que E tem boa redução. Então

- Se $a_p(E) \not\equiv 0 \pmod{p}$, E tem redução ordinária em p ;
- Se $a_p(E) \equiv 0 \pmod{p}$, E tem redução supersingular em p .^[122]

Prova. Note que, pela recorrência (3.1), $a_{p^e}(E) \equiv a_p(E)^e \pmod{p}$ para todo $e \geq 1$. Logo, se $a_p(E) \equiv 0 \pmod{p}$, então, para todo e , $a_{p^e}(E) = p^e + 1 - \# \tilde{E}(\mathbb{F}_{p^e}) \equiv 0 \pmod{p} \implies \# \tilde{E}(\mathbb{F}_{p^e}) \not\equiv 0 \pmod{p}$.

Reciprocamente, se $a_p(E) \not\equiv 0 \pmod{p}$, pelo Pequeno Teorema de Fermat, $a_p(E)^{p-1} \equiv 1 \pmod{p} \implies a_{p^{p-1}}(E) = p^{p-1} + 1 - \# \tilde{E}(\mathbb{F}_{p^e}) \equiv 1 \pmod{p} \implies \# \tilde{E}(\mathbb{F}_{p^{p-1}}) \equiv 0 \pmod{p}$. Logo, $a_p(E) \equiv 0 \pmod{p} \iff \# \tilde{E}(\mathbb{F}_{p^e}) \not\equiv 0 \pmod{p}$ para todo $e \geq 1$. Pelo Teorema 2.1.11, isto é equivalente a $\# \tilde{E}(\mathbb{F}_{p^e}) \cap \tilde{E}[p] = \{O\}$ para todo $e \geq 1$, o que só pode ocorrer se, e somente se, $\tilde{E}[p] = \{O\}$, isto é, E tem redução supersingular em p . ■

^[119]onde a função de Hasse–Weil *não* é dada nem por aquela série nem pelo produto de Euler!

^[120]Esta foi a motivação para a definição das L -funções de Dirichlet. Para mais informações, veja (SERRE, 1973, Capítulo 6).

^[121]Veja também Hsu e Miller (2003), Apêndice B, para um algoritmo em PARI/GP para calcular posto analítico.

^[122]Se $p \geq 5$, segue do Teorema de Hasse–Weil (Teorema 1.1.5) que $a_p(E) \equiv 0 \pmod{p} \iff a_p(E) = 0$.

Revisitemos o exemplo 2.2.4. Pelo Teorema da Modularidade (Teorema 3.2.3), existe uma autoforma $f \in \mathbb{S}_2(\Gamma_0(N_E))$ tal que $a_p(E) = a_p(f)$ para todo p . Para todo $p < 100$, os únicos coeficientes $a_p(f)$ nulos da autoforma f (LMFDB 30.2.a.a) ocorrem em $p \in \{23, 47, 59, 71\}$. Logo, dentre os primos $p < 100$, E só possui redução supersingular nos primos listados acima.

Toda curva elíptica E sobre $\mathbb{Q}$ possui um modelo na forma $y^2 = x^3 + ax + b$.^[123] Para este caso, temos outra forma de distinguir os tipos de redução boa:

Proposição 3.2.6. Suponha $p \geq 3$ ^[124]. Então, E tem redução supersingular em p se, e somente se, p divide o coeficiente de x^{p-1} em $(x^3 + ax + b)^{(p-1)/2}$.

Prova. Em vista do critério anterior, basta mostrarmos que o coeficiente de x^{p-1} em $(x^3 + ax + b)^{(p-1)/2}$ é, de fato, $a_p(E)$.

Observe que o mapa $\chi: \mathbb{F}_p^\times \rightarrow \{\pm 1\}$ dado por

$$\chi(\alpha) = \begin{cases} 1, & \text{se } \alpha \text{ é quadrado} \\ -1, & \text{caso contrário} \end{cases}$$

é um morfismo de grupos. Como $\mathbb{F}_p^\times$ é cíclico de ordem $p-1$, este morfismo também pode ser expresso como

$$\chi(\alpha) = \alpha^{(p-1)/2}.$$

Estenda a notação para 0 fazendo $\chi(0) = 0$. Note que $1 + \chi(\alpha)$ é o número de soluções da equação $y^2 = \alpha$, donde^[125]

$$\begin{aligned} \#E(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3 + \bar{a}x + \bar{b})) = 1 + p + \sum_{x \in \mathbb{F}_p} (x^3 + \bar{a}x + \bar{b})^{(p-1)/2} \\ &\implies -a_p(E) = \sum_{x \in \mathbb{F}_p} (x^3 + \bar{a}x + \bar{b})^{(p-1)/2}. \end{aligned}$$

Vamos computar esta soma. Observe que elevar os elementos de $\mathbb{F}_p$ à i -ésima potência, com $p-1 \nmid i$, apenas os permuta, donde $\sum_{x \in \mathbb{F}_p} x^i = 0$. No outro caso, $p-1 \mid i$, é fácil ver que

$\sum_{x \in \mathbb{F}_p} x^i = -1$. Como os expoentes x^n que aparecem na expansão de $(x^3 + \bar{a}x + \bar{b})^{(p-1)/2}$ são

^[123]Como veremos no capítulo 5, podemos supor que esse modelo é p -minimal para todo $p \geq 5$ (um modelo *quase* minimal global!).

^[124]Não vamos precisar do caso $p = 2$, mas, só por curiosidade, E terá redução supersingular módulo 2 se, e somente se, $j(\tilde{E}) = 0$. Isso segue das possibilidades para a equação de Weierstrass de uma curva elíptica em característica 2, discutidas em Washington (2008), seção 2.8.

^[125]Não se esqueça do ponto no infinito!

$0 \leq n \leq \frac{3}{2}(p-1)$, o único n múltiplo de $p-1$ é o próprio $n = p-1$. Logo,

$$\sum_{x \in \mathbb{F}_p} (x^3 + \bar{a}x + \bar{b})^{(p-1)/2} = \sum_{i=0}^{p-2} A_i \sum_{x \in \mathbb{F}_p} x^i + A_{p-1} \underbrace{\sum_{x \in \mathbb{F}_p} x^{p-1}}_{=-1} + \sum_{i=p}^{3(p-1)/2} A_i \sum_{x \in \mathbb{F}_p} x^i = -a_p(E)$$

$$\implies A_{p-1} \equiv a_p(E) \pmod{p}. \quad \blacksquare$$

3.3 A Conjectura de Birch e Swinnerton-Dyer

A Conjectura BSD sugere que a relação entre os postos algébrico e analítico ultrapassa a semelhança entre seus nomes:

Conjectura BSD (Birch e Swinnerton-Dyer^[126]). Seja E uma curva elíptica sobre $\mathbb{Q}$. Então, os postos algébrico e analítico de E são iguais (BIRCH; SWINNERTON-DYER, 1965).

Em particular, $r_{\text{alg}}(E) \neq 0$ se, e somente se, $r_{\text{an}}(E) \neq 0$, ou seja, se $L(1, E) = 0$ se, e somente se, E tem infinitos pontos racionais (a recíproca desta afirmação já foi provada por Coates e Wiles (1977) para certas curvas elípticas com multiplicação complexa^[127], e por Gross e Zagier (1986) no caso geral^[128]).

O motivo pelo qual a Conjectura BSD é tão importante é que ela relaciona $r_{\text{alg}}(E)$, um objeto difícil de calcular, a $r_{\text{an}}(E)$, um objeto fácil de calcular. Assim, a importância da Conjectura BSD provém da importância do próprio posto algébrico na compreensão das curvas elípticas sobre $\mathbb{Q}$.

3.3.1 Computando o grupo de uma curva elíptica

Como vimos na seção 3.1, o grupo de pontos $\mathbb{Q}$ -racionais de uma curva elíptica é constituído de uma parte de torção bem compreendida, e de uma parte livre ainda envolta em incerteza. Esta disparidade se verifica ao computar o grupo na prática: a parte de torção tende a ser relativamente fácil, enquanto não existem métodos garantidos para encontrar o posto algébrico de uma curva elíptica qualquer!

^[126]Este enunciado também é conhecido como a versão *fraca* da Conjectura BSD, em contraste com a versão *forte* apresentada no Apêndice A.1. No entanto, este é o enunciado da conjectura de Birch e Swinnerton-Dyer como Problema do Milênio. Por isso, tomaremos esta versão como *default*.

^[127]Em geral o grupo de endomorfismos de uma curva elíptica é composto pelas isogenias de multiplicação por inteiro. Curvas elípticas que possuem endomorfismos extras são ditas possuir **multiplicação complexa**. Mais especificamente, o teorema de Coates–Wiles vale para curvas elípticas com multiplicações complexas definidas sobre um corpo quadrático imaginário de número de classe 1 (veja Neukirch (2009), p. 34, seção I.6 para mais informações sobre número de classe, e p. 37 para a lista completa de tais corpos).

^[128]Originalmente, para toda curva elíptica *modular*, isto é, que satisfizesse a Conjectura de Taniyama–Shimura (Teorema da Modularidade, Teorema 3.2.3).

3.3.1.1 Computando o subgrupo de torção

Dissemos que computar o subgrupo de torção é relativamente simples. De fato, o resultado seguinte transforma a busca por pontos de torção em algo computável em tempo finito:

Teorema 3.3.1 (Nagell–Lutz, 1935-37). Seja $E: y^2 = x^3 + ax + b$ uma curva elíptica sobre $\mathbb{Q}$, com $a, b \in \mathbb{Z}$. Se $P = (x, y) \in E(\mathbb{Q})$ é de torção, então $x, y \in \mathbb{Z}$. Além disso, $y = 0$ ^[129] ou $y^2 | (4a^3 + 27b^2)$ (WASHINGTON, 2008, p. 205, Teorema 8.7).

Assim, se pudermos fatorar o discriminante $4a^3 + 27b^2 = -\Delta(E)/16$, obtemos uma lista de pontos de E na qual certamente estão contidos todos os pontos de torção afins^[130]. Porém, o Teorema de Nagell–Lutz *não* é uma equivalência: um ponto de coordenadas inteiras com $y^2 | (4a^3 + 27b^2)$ pode muito bem ser um ponto de ordem infinita!^[131] Sabemos pelo Teorema de Mazur (Teorema 3.1.2) que um ponto de torção tem ordem no máximo 12, o que nos dá um critério para saber se um ponto é ou não de torção. Como somar um ponto consigo mesmo 12 vezes pode ser custoso computacionalmente, o seguinte critério, que é uma consequência imediata do Teorema de Nagell–Lutz, pode ser útil:

Corolário 3.3.2. Seja $E: y^2 = x^3 + ax + b$ uma curva elíptica sobre $\mathbb{Q}$, com $a, b \in \mathbb{Z}$. Se alguma das coordenadas de $P \in E(\mathbb{Q})$ não é inteira, então P tem ordem infinita.

Exemplo 3.3.3. Seja $E: y^2 = x^3 + 3x$ (LMFDB 288.a2), cujo discriminante é $-1728 = -2^6 \cdot 3^3$. Pelo Teorema de Nagell–Lutz, os pontos candidatos a torção satisfazem $y \in \{0, 2, 3, 6\}$, o que corresponde aos pontos

$$(0, 0), (1, 2) \text{ e } (3, 6).$$

O ponto $(0, 0)$ é de ordem 2. Note que

$$x([2](1, 2)) = \frac{1}{4} \quad \text{e} \quad x([2](3, 6)) = \frac{121}{104},$$

donde $(1, 2)$ e $(3, 6)$ são de ordem infinita.

Limitações computacionais de lado, calcular o subgrupo de torção é, portanto, um problema resolvido. O próximo passo é calcular o posto algébrico.

^[129]Isto é, P é um ponto de ordem 2.

^[130]E, por isso, o “relativamente” antes do “fácil”... Se for muito grande, pode ser difícil fatorá-lo e, portanto, listar os candidatos a pontos de torção. Existem algoritmos para contornar este problema. Por exemplo, veja Washington (2008), p. 302, seção 9.3, para uma descrição do Algoritmo de Doud, que observa a curva elíptica como uma curva sobre $\mathbb{C}$ e utiliza técnicas analíticas para encontrar os pontos no toro que correspondem aos pontos de coordenadas inteiras na curva.

^[131]Além disso, ninguém está dizendo que se um ponto tiver coordenadas inteiras, então $y = 0$ ou $y^2 | (4a^3 + 27b^2)$: a curva elíptica $E: y^2 = x^3 + 9x$ (LMFDB 576.c4) possui discriminante $-46656 = -2^6 \cdot 3^6$, mas o ponto (de ordem infinita, evidentemente) $(4, 10) \in E(\mathbb{Q})$ tem coordenadas inteiras e $y^2 \nmid (-46656)/(-16) = 2916$.

3.3.1.2 Computando o posto algébrico

E é aqui onde se encontram as maiores dificuldades em se computar o grupo de uma curva elíptica: como comentamos anteriormente, não existe um método garantido para calcular o posto algébrico de uma curva elíptica qualquer! Na prática, aborda-se este problema das seguintes maneiras^[132]:

- Se você tiver muita sorte, determinar todas as soluções integrais de sua curva elíptica pode ser feito usando técnicas de Teoria (até mesmo Elementar) dos Números^[133], ou o problema de calcular o posto algébrico pode se reduzir a um resultado (não necessariamente trivial) que garanta a resposta procurada^[134]. Em geral, curvas elípticas “sortudas” assim têm posto baixo^[135].
- Se é conhecida uma cota superior para o posto algébrico da curva elíptica em questão, pode-se tentar encontrar pontos racionais de ordem infinita até atingir esta cota^[136]. Porém, se a sua cota superior for estritamente maior que o posto (o que pode ser difícil de saber), não vai adiantar continuar procurando os pontos racionais de ordem infinita independentes que faltam: eles simplesmente não vão existir.
- A prova do Teorema de Mordell-Weil é não-construtiva. Porém, há um algoritmo para calcular posto algébrico, baseado na essência desta prova, que supostamente funciona para qualquer curva elíptica. O problema é que não se sabe se este algoritmo sempre termina (pelo menos, todas as vezes que este algoritmo foi usado até hoje, ele terminou^[137])! O *software* mwrank, implementado por Cremona, utiliza este algoritmo para (tentar) calcular o posto algébrico^[138].

Se a conjectura de Birch e Swinnerton-Dyer for verdadeira, pode-se computar o posto^[139]

^[132]Além destas maneiras listadas, outra frequentemente mais cômoda quando trabalhando com exemplos concretos, é ver se a sua curva elíptica já não está indexada, por exemplo, no LMFDB ou no banco de dados de Cremona (2019a)!

^[133]Por exemplo, em Martinez *et al.* (2013), p. 161, Exemplo 4.26, encontram-se todos os pontos racionais da curva elíptica $y^2 = x^3 - 432$ (e conclui-se que seu posto é 0) apelando ao caso $n = 3$ do Último Teorema de Fermat!

^[134]Veja a seção 4.3.2 para um exemplo de resultado poderoso que pode determinar de vez o posto da curva quando este é 0 ou 1 (Teorema 4.3.17).

^[135]Quanto à isso, parece que curvas elípticas sobre $\mathbb{Q}$ tendem a ter postos baixos, mesmo. Veja a subseção 5.1.3 para mais detalhes.

^[136]A principal maneira conhecida de se limitar superiormente o posto algébrico de uma curva elíptica envolve o uso dos grupos de Selmer, provenientes da co-homologia de Galois. Veja uma descrição na subseção 4.3.3.

^[137]Se este algoritmo parece sempre terminar, por que não aplicá-lo à curva elíptica de Elkies e determinar de uma vez por todas se seu posto é 28 ou não? Aqui entram, novamente, as limitações dos computadores: o condutor da curva elíptica de Elkies é enorme e, em geral, quanto maior o condutor, mais difícil é para o computador lidar com a curva. Veja a thread <<https://math.stackexchange.com/questions/812363/exact-rank-of-elkies-curve>> para uma discussão.

^[138]Este *software* também computa outras coisas, como condutores, torção, *twists* isomorfos sobre corpos quadráticos, entre outras coisas. Veja a página web de Cremona (2019b) para mais informações.

^[139]analítico ou algébrico, pois seriam o mesmo!

de uma curva elíptica E da seguinte forma^[140]: pela busca computacional de pontos independentes de ordem infinita, obtêm-se cotas inferiores cada vez maiores para $r_{\text{alg}}(E)$. Por outro lado, como comentamos anteriormente, pode-se computar a k -ésima derivada de $L(E, s)$ em $s = 1$ com a precisão que se deseja, obtendo-se cotas superiores cada vez menores para $r_{\text{an}}(E)$. Como a conjectura implica que $r_{\text{alg}}(E) = r_{\text{an}}(E)$, eventualmente as estimativas se cruzarão, revelando o valor do posto de E .

3.3.1.3 Computando os geradores de $E(\mathbb{Q})$

Se sabemos como calcular o posto algébrico r de E , o grupo todo $E(\mathbb{Q})$ é computável. Considere a função de **altura canônica de Néron–Tate**, definida por

$$\hat{h}(P) = \lim_{n \rightarrow \infty} \frac{h_x(2^n P)}{4^n}.$$

Esta função é uma forma quadrática não-degenerada, e $\hat{h}(P) = 0 \iff P \in E(\mathbb{Q})_{\text{tor}}$ (ver seção A.1.1).

O primeiro passo para computar $E(\mathbb{Q})$ é encontrar geradores para $E(\mathbb{Q})/2E(\mathbb{Q})$, que já sabemos ser finito, pelo Teorema fraco de Mordell–Weil (Teorema 3.1.11). Buscamos r pontos independentes $P_1, \dots, P_r$ de ordem infinita e checamos se existe alguma soma de P_i que dá $2Q$ para algum $Q \in E(\mathbb{Q})$. Neste caso, trocamos algum destes P_i da soma por Q , e o índice do subgrupo gerado por eles cai pela metade, se aproximando de $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$. Após finitos passos (pois $E(\mathbb{Q})$ é finitamente gerado), obteremos P_i também independentes módulo 2 e que, portanto, geram $E(\mathbb{Q})/2E(\mathbb{Q})$.

O próximo passo usa a seguinte proposição:

Proposição 3.3.4 (Zagier). Seja $B \in \mathbb{R}_{>0}$ tal que $S(B) = \{P \in E(\mathbb{Q}) / \hat{h}(P) \leq B\}$ contém um conjunto de geradores de $E(\mathbb{Q})/2E(\mathbb{Q})$. Então, S gera $E(\mathbb{Q})$ (STEIN, 2016, p. 4, Lema 1.4).

Logo, tomando $B = \max\{\hat{h}(P_1), \dots, \hat{h}(P_r)\}$, segue da proposição anterior que $S(B)$ gera $E(\mathbb{Q})$. Porém, é difícil computar pontos por suas alturas canônicas: é mais fácil usar a altura logarítmica. Um resultado de Cremona–Pricket–Siksek (CREMONA, 1997, p. 77, Proposição 3.5.1) nos dá uma cota explícita para a diferença entre estas duas alturas de um ponto, isto é, existe C , que só depende de E , tal que $|\hat{h}(P) - h_x(P)| < C$ para todo $P \in E(\mathbb{Q})$. Assim, tomando $A = B + C$, usamos a altura logarítmica para computar $\{P \in E(\mathbb{Q}) / h_x(P) \leq A\}$, que conterá $S(B)$ e, portanto, um conjunto de geradores para a parte livre de $E(\mathbb{Q})$.

Para mais detalhes sobre os aspectos computacionais das curvas elípticas, bem como algoritmos explícitos para as computações descritas acima, referimos o leitor ao já mencionado livro de Cremona (1997).

^[140]Seguindo os roteiros apresentados por Stein (2016), p. 3, seção 1.2, e Cremona (1997).

3.4 Representações de Galois

Seja G um grupo. Uma **representação** de G é um morfismo de grupos $\rho : G \rightarrow \mathrm{GL}(V)$, onde V é um espaço vetorial de dimensão finita. Dizemos que ρ é **irreduzível** se

se W é um subespaço de V tal que W é fechado pela ação de $\rho(G)$, então $W = 0$.

Definição 3.4.1. Seja ℓ primo. Uma **representação de Galois** ℓ -ádica é uma representação contínua^[141] $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$.

Duas representações de Galois ρ_1 e ρ_2 são **equivalentes** ($\rho_1 \sim \rho_2$) se existe $m \in \mathrm{GL}_2(\mathbb{Q}_\ell)$ tal que $\rho_2(\sigma) = m^{-1}\rho_1(\sigma)m$, para todo $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Seja p primo. Recorde que os elementos de Frobenius em $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ estão definidos a menos de $I_{\mathfrak{p}}$, onde $\mathfrak{p} \in \mathrm{Specm}(\overline{\mathbb{Z}})$ é um ideal sobre p .

Definição 3.4.2. Seja p primo. Uma representação de Galois ℓ -ádica é **não-ramificada** em p se $I_{\mathfrak{p}} \subseteq \ker(\rho)$ para qualquer $\mathfrak{p} \in \mathrm{Specm}(\overline{\mathbb{Z}})$ sobre p . Caso contrário, é dita **ramificada**.

Isto significa que, apesar de $\mathrm{Frob}_{\mathfrak{p}}$ poder não estar unicamente definido, $\rho(\mathrm{Frob}_{\mathfrak{p}})$ pode estar bem-definido, que é o que ocorre quando ρ não é ramificada em p . Como o conjunto dos elementos de Frobenius é denso em $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (Teorema 1.6.5) e ρ é contínua, a imagem de ρ fica bem definida nos elementos de Frobenius para os primos nos quais ρ não ramifica.

Seja E uma curva elíptica sobre $\mathbb{Q}$ e ℓ primo. Considere os subgrupos de ℓ^n -torção $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ e os mapas $E[\ell^{n+1}] \rightarrow E[\ell^n]$ de multiplicação por ℓ .

Definição 3.4.3. O **módulo de Tate** ℓ -ádico de E é o limite inverso

$$\mathrm{Ta}_\ell(E) = \varprojlim_{n \in \mathbb{N}} E[\ell^n] \cong \mathbb{Z}_\ell^2.$$

A extensão finita $\mathbb{Q}(E[\ell^n])/\mathbb{Q}$ é Galois e temos um mapa de restrição

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\rightarrow \mathrm{Aut}(E[\ell^n]), \\ \sigma &\mapsto \sigma|_{E[\ell^n]} \end{aligned}$$

que é compatível com os mapas de multiplicação por ℓ . Logo, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ age sobre

$$\mathrm{Aut}(\mathrm{Ta}_\ell(E)) \cong \varprojlim \mathrm{Aut}(E[\ell^n]) \cong \varprojlim \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Definição 3.4.4. A representação de Galois ℓ -ádica da curva elíptica E é o mapa

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{Aut}(\mathrm{Ta}_\ell(E)) \subseteq \mathrm{GL}_2(\mathbb{Q}_\ell).$$

^[141]Com a topologia de Krull no domínio e a topologia p -ádica no contradomínio.

Teorema 3.4.5. A representação $\rho_{E,\ell}$ é irredutível e não-ramificada em todo primo $p \nmid \ell N_E$.

Ideias da Prova. A irredutibilidade de $\rho_{E,\ell}$ segue do fato de E não possuir multiplicação complexa (cf. nota [127], já que um tal endomorfismo não poderia estar definido sobre $\mathbb{Q}$). Veja Serre (1989), p. IV-9, para uma demonstração deste fato.

Seja $p \nmid \ell N_E$ e $\mathfrak{p} \in \text{Specm}(\overline{\mathbb{Z}})$ sobre p . Então E tem redução boa em p . Nesse caso, para todo $n \geq 1$, $E[\ell^n] \cong \tilde{E}[\ell^n]$ [142]. Pelo diagrama comutativo

$$\begin{array}{ccc} D_{\mathfrak{p}} & \longrightarrow & \text{Aut}(E[\ell^n]) \\ \downarrow \text{mod } p & & \downarrow \text{mod } p \\ \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) & \longrightarrow & \text{Aut}(\tilde{E}[\ell^n]), \end{array}$$

a ação de $I_{\mathfrak{p}} \subseteq D_{\mathfrak{p}}$ sobre $\text{Aut}(E[\ell^n])$ é trivial, para todo n . Logo, $I_{\mathfrak{p}} \subseteq \ker(\rho_{E,\ell})$. $\square$

3.4.1 Representações de Galois Residuais

Por definição, a imagem de $\rho_{E,\ell}$ está contida em $\text{GL}_2(\mathbb{Z}_{\ell})$. Recorde que $\mathbb{Z}_{\ell}/\ell\mathbb{Z}_{\ell} \cong \mathbb{F}_{\ell}$. Compondo $\rho_{E,\ell}$ com a projeção $\text{GL}_2(\mathbb{Z}_{\ell}) \twoheadrightarrow \text{GL}_2(\mathbb{F}_{\ell})$, obtemos a **representação de Galois residual** ℓ -ádica de E denotada $\bar{\rho}_{E,\ell}: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_{\ell})$.

Pelo Teorema 2.1.11, $E[\ell] \cong \mathbb{F}_{\ell}^2$. Logo, podemos ver $E[\ell]$ como um $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -módulo, e $E(\mathbb{Q})[\ell]$ é o submódulo fixo pela ação dada por $\bar{\rho}_{E,\ell}$.

Proposição 3.4.6. A representação residual $\bar{\rho}_{E,\ell}$ é irredutível se, e somente se, $E(\mathbb{Q})[\ell]$ é trivial.

Demonstração. Se $\bar{\rho}_{E,\ell}$ é irredutível, é claro que $E(\mathbb{Q})[\ell] = 0$. Por outro lado, se $E(\mathbb{Q})[\ell] = 0$, então todo automorfismo de $E[\ell]$ pode ser visto como um elemento do grupo de Galois $\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ impondo que $\mathbb{Q}$ seja fixado [143]. Logo, a ação dada por $\bar{\rho}_{E,\ell}$ é transitiva e $\bar{\rho}_{E,\ell}$ é irredutível. $\blacksquare$

Observação 3.4.7. Como $\ker(\rho_{E,\ell}) \subseteq \ker(\bar{\rho}_{E,\ell})$, se $\rho_{E,\ell}$ não ramifica em p , então $\bar{\rho}_{E,\ell}$ não ramifica em p . Em particular, $\bar{\rho}_{E,\ell}$ não ramifica em $p \nmid \ell N_E$. A seguinte proposição trata de (quase todos) os demais casos:

Proposição 3.4.8. Seja $p \neq \ell$ primo e suponha que E tem redução multiplicativa em p . Então, $\bar{\rho}_{E,\ell}$ ramifica em p se, e somente se, $\ell \nmid v_p(\Delta(E))$.

[142] Este resultado é uma consequência do Critério de Néron–Ogg–Shafarevich (HUSEMÖLLER, 2004, p. 280, seção 14.3). Porém, o nosso caso é simples: basta checarmos que o mapa de redução é injetor sobre $E[\ell^n]$, e isto segue da Proposição 4.3.9 adiante.

[143] Se existisse um elemento racional não-trivial em $E[\ell]$, não seria possível, por exemplo, transformar o automorfismo $x \mapsto -x$ em um elemento do grupo de Galois, pois não fixaria $E(\mathbb{Q})[p]$.

Prova. Seja p tal que $v_p(\Delta(E)) > 0$ e suponha que E tem redução multiplicativa *split* em p . Então, $\bar{\rho}_{E,\ell}$ ramifica em p se, e somente se, I_p age trivialmente em $E[\ell]$, para cada $\mathfrak{p} \in \text{Specm}(\bar{\mathbb{Z}})$. Isto, por sua vez, é equivalente a $\mathfrak{p} \cap \mathbb{Q}(E[\ell])$ não ramificar na extensão $\mathbb{Q}(E[\ell])/\mathbb{Q}$, pois a ordem do grupo de inércia de $\mathfrak{p} \cap \mathbb{Q}(E[\ell])$ é exatamente seu índice de ramificação. Como ramificação de primos é uma propriedade local, podemos trocar aquela extensão por $\mathbb{Q}_p(E[\ell])/\mathbb{Q}_p$.

Vamos entender o que é ramificação no contexto de corpos p -ádicos. Considere uma extensão Galois finita $(L, w)/(K, v)$. Se π_K e π_L são parâmetros locais para K e L , respectivamente, temos que $\pi_K = \alpha\pi_L^e$, para algum $\alpha \in L$ tal que $|\alpha|_w = 1$ e $e \in \mathbb{Z}$. Assim, temos um equivalente p -ádico da igualdade fundamental para corpos de números:

$$[L : K] = e[l_w : k_v].$$

Se $e = 1$, dizemos que a extensão **não ramifica**.^[144]

Como E tem redução multiplicativa *split*, pelo Teorema da Uniformização p -ádica (Teorema 2.4.5 e Proposição 2.4.6), $E(\bar{\mathbb{Q}}_p) \cong \bar{\mathbb{Q}}_p^\times / q^\mathbb{Z}$ para algum $q \in \mathbb{Q}_p$ tal que $|q|_p < 1$. Logo, $E[\ell] = (\bar{\mathbb{Q}}_p^\times / q^\mathbb{Z})[\ell] = \langle \mu_\ell, q^{1/\ell} \rangle / q^\mathbb{Z}$, onde μ_ℓ é uma raiz ℓ -ésima primitiva da unidade e $q^{1/\ell} \in \bar{\mathbb{Q}}_p$ é uma raiz ℓ -ésima de q . Logo, podemos passar a considerar a extensão $\mathbb{Q}_p(\mu_\ell, q^{1/\ell})/\mathbb{Q}_p$. Como a extensão $\mathbb{Q}_p(\mu_\ell)/\mathbb{Q}_p$ não ramifica^[145], usando a multiplicatividade do grau de extensão, $\mathbb{Q}_p(\mu_\ell, q^{1/\ell})/\mathbb{Q}_p$ ramifica se, e somente se, $\mathbb{Q}_p(\mu_\ell, q^{1/\ell})/\mathbb{Q}_p(\mu_\ell)$ o faz. Logo, para concluir a prova, vamos mostrar que isto é equivalente a $\ell \nmid v_p(q)$. Note que $v_p(q) = v_p(\Delta(E_q)) = v_p(\Delta(E)) > 0$.

Para simplificar a notação, faça $L = \mathbb{Q}_p(\mu_\ell, q^{1/\ell})$, $K = \mathbb{Q}_p(\mu_\ell)$ e tome parâmetros locais π_L e π_K , respectivamente, para estes corpos. Como $K/\mathbb{Q}_p$ não ramifica, $v_p(\pi_K) = 1$. Seja w a extensão de v_p para L . Observe que

$$1 = w(\pi_K) = w(\alpha\pi_L^e) = \cancel{w(\alpha)}^0 + e \cdot w(\pi_L) \implies w(\pi_L) = \frac{1}{e}.$$

Temos que $q^{1/\ell} = \alpha'\pi_L^\beta$ para algum $\beta \in \mathbb{Z}_{>0}$ e $\alpha' \in L$ tal que $w(\alpha') = 0$. Logo, $v(q) = \frac{\beta\ell}{e}$.

Como $e \mid \ell$ primo, $e = 1$ ou $e = \ell$. Se $e = 1$, isto é, a extensão não ramifica, é claro que $\ell \mid v_p(q)$. Seja $e = \ell$ e suponha que $\ell \nmid v_p(q) = \beta$. Como $q^{1/\ell}$ gera a extensão, podemos escrever

$$\pi_L = \sum_{i=0}^{\ell-1} a_i q^{i/\ell} \implies w(\pi_L) = \frac{1}{\ell} \geq \min_{0 \leq i \leq \ell-1} \left\{ v(a_i) + \frac{i\beta}{\ell} \right\}.$$

Como $a_i \in \mathcal{O}_K$ e a extensão $K/\mathbb{Q}_p$ não ramifica, para todo i , $v(a_i) \in \mathbb{Z}_{\geq 0}$. Logo, todos os elementos do conjunto minimalizado são inteiros não-negativos. Logo, como esse mínimo é um inteiro não-negativo limitado por $1/\ell$, esse mínimo é 0.

^[144]Note que esta definição é “compatível” com a definição que fizemos de ramificação em corpos de números: se $\mathbb{L}/\mathbb{K}$ é uma extensão Galois finita de corpos de números e $\mathfrak{P} \in \text{Specm}(\mathbb{L})$ é um primo sobre $\mathfrak{p} \in \text{Specm}(\mathbb{K})$ com índice de ramificação e , a extensão $(\mathbb{L}, v_{\mathfrak{P}})/(\mathbb{K}, v_{\mathfrak{p}})$ não ramifica no sentido acima se, e somente se, $e = 1$, pois, pela igualdade fundamental, $[\mathbb{L} : \mathbb{K}] = [\mathbb{L}_{\mathfrak{P}} : \mathbb{K}_{\mathfrak{p}}] = e[l_{\mathfrak{P}} : k_{\mathfrak{p}}]$.

^[145]Como $\text{mdc}(p, \ell) = 1$, pelo Lema de Hensel (Teorema 1.4.15), $\text{Gal}(\mathbb{Q}_p(\mu_\ell)/\mathbb{Q}_p) \cong \text{Gal}(\mathbb{F}_p(\mu_\ell)/\mathbb{F}_p)$.

Como π_L não é um invertível, existe $i > 0$ tal que $a_i \neq 0$, e também $v(a_0) \neq 0$. Logo, o mínimo é atingido em certo $i_0 > 0$, de modo que

$$v(a_{i_0}) + \frac{i_0 \beta}{\ell} = 0 \implies \beta = 0,$$

o que não pode ocorrer. Logo, se $e = \ell$, $\ell \nmid v_p(q)$, concluindo a prova da afirmação neste caso.

Se a redução de E em p é multiplicativa não-*split*, a extensão $\mathbb{Q}_p(\sqrt{\gamma_{\mathbb{Q}_p}(E)})/\mathbb{Q}_p$ não ramifica^[146], em que E tem redução multiplicativa *split*. Logo, podemos reduzir este caso ao anterior, concluindo a prova. ■

^[146]Por hipótese, $X^2 - \gamma_{\mathbb{Q}_p}(E)$ não tem raiz em $\mathbb{Q}_p$. Pelo Lema de Hensel (Teorema 1.4.15), também não tem raiz em $\mathbb{F}_p$, donde $[\mathbb{F}_p(\sqrt{\gamma_{\mathbb{Q}_p}(E)}) : \mathbb{F}_p] = 2 = [\mathbb{Q}_p(\sqrt{\gamma_{\mathbb{Q}_p}(E)}) : \mathbb{Q}_p]$.

GRUPOS DE SELMER E GRUPOS DE TATE–SHAFAREVICH

O grupo de Tate–Shafarevich é o tapete para debaixo do qual os especialistas em teoria dos números varrem todas as dificuldades do cálculo de pontos racionais de curvas elípticas (CIPRA, 2004, p. 16).

4.1 Espaços homogêneos e grupos de Weil–Châtelet

Seja K uma extensão qualquer de $\mathbb{Q}$.^[147]

Definição 4.1.1. Um **espaço homogêneo** para E é um par (C, μ) , onde C é uma curva algébrica não-singular sobre K e $\mu: C \times E \rightarrow C$ é um K -morfismo satisfazendo:

- (i) $\mu(p, O) = p$, para todo $p \in C$;
- (ii) $\mu(\mu(p, P), Q) = \mu(p, P + Q)$, para todo $p \in C, P, Q \in E$.
- (iii) Dados $p, q \in C$, existe um único $P \in E$ tal que $\mu(p, P) = q$.^[148]

Note que μ se parece com uma adição: a propriedade (i) diz que $O \in E$ é como se fosse um elemento neutro, (ii) parece com a associatividade, e (iii) nos diz que é possível definir uma operação inversa, semelhante à subtração. Por isto, às vezes a notação $\mu(p, P)$ será simplificada para $p + P$.

A “subtração” que mencionamos é o mapa $v: C \times C \rightarrow E$ tal que $v(p, q)$ é o único $P \in E$ com $\mu(p, P) = q$, conforme (iii), e a sua notação também será simplificada para $p - q$. Outras propriedades destes mapas estreitam a analogia entre μ e a adição, e v e a subtração:

^[147]A referência principal deste capítulo é o livro de Silverman (2009), onde o leitor pode encontrar uma discussão mais completa do assunto.

^[148]Isto é, μ é uma ação de grupo algébrico ((i) e (ii)) simplesmente transitiva ((iii)), e de onde vem o nome “homogêneo”.

Lema 4.1.2. Com a notação anterior^[149], para todo $p, q \in C$ e $P, Q \in E$,

- $p + O = p$ e $p - O = p$;
- $p + (q - p) = q$ e $(p + P) - p = P$;
- $(q + Q) - (p + P) = (q - p) + (Q - P)$.

Seja $p_0 \in C$ e considere o mapa de “translação por p_0 ” $\theta : E \rightarrow C$ dado por $\theta(P) = p_0 + P$. Assim como é intuitivo que μ atue como uma soma, é intuitivo que θ seja, na verdade, um isomorfismo:

Proposição 4.1.3. Sejam C um espaço homogêneo para E , $p_0 \in C$ e o mapa $\theta : E \rightarrow C$ dado por $\theta(P) = p_0 + P$. Então, θ é um isomorfismo de curvas algébricas definido sobre $K(p_0)$, a menor extensão de K sobre a qual p_0 é racional^[150]. Em particular, C é um *twist* de E .

Prova. Seja $\sigma \in \text{Gal}(K/K(p_0))$. Como a ação de E sobre C é um K -morfismo,^[151]

$$\theta(P)^\sigma = (p_0 + P)^\sigma = p_0^\sigma + P^\sigma = p_0 + P^\sigma = \theta(P^\sigma),$$

donde θ está definido sobre $K(p_0)$. Como E age transitivamente sobre C , θ é uma bijeção. Logo, o *pushforward* induzido θ_* é um isomorfismo entre $K(E)$ e $K(C)$ e, portanto, E e C são birracionalmente equivalentes por θ . Sendo ambas as curvas não-singulares, θ é um isomorfismo. ■

Corolário 4.1.4. Para todo $p, q \in C$ e $P \in E$,

$$p + P = \theta(\theta^{-1}(p) + P) \quad \text{e} \quad q - p = \theta^{-1}(q) - \theta^{-1}(p).$$

Em outras palavras, a “adição” μ e a “subtração” ν são caracterizadas pelo isomorfismo θ .

Prova. Basta usar que $\theta^{-1}(p) = \nu(p, p_0)$. ■

Corolário 4.1.5. A “subtração” ν é um K -morfismo.

Prova. A subtração de E é um K -morfismo. Dado $\sigma \in \text{Gal}(\bar{K}/K)$, pelo terceiro item do Lema 4.1.2,

$$\begin{aligned} (q - p)^\sigma &= (\theta^{-1}(q) - \theta^{-1}(p))^\sigma \\ &= \theta^{-1}(q)^\sigma - \theta^{-1}(p)^\sigma \\ &= (p_0 + \theta^{-1}(q))^\sigma - (p_0 + \theta^{-1}(p))^\sigma \\ &= q^\sigma - p^\sigma, \end{aligned}$$

^[149]Cuidado! Os sinais $+$ e $-$ representam coisas diferentes, dependendo dos objetos envolvidos.

^[150]Em outras palavras, a extensão gerada pelas coordenadas de p_0 .

^[151]O grupo de Galois age num ponto coordenada-a-coordenada.

onde $v: C \times C \rightarrow E$ está definido sobre K e, como a subtração de E e θ são K -morfismos, v também é. ■

Definição 4.1.6. Dois espaços homogêneos C_1 e C_2 para E definidos sobre K são **equivalentes** se existe um isomorfismo $\theta: C_1 \rightarrow C_2$ compatível com as ações μ_1 e μ_2 de E sobre estas curvas, isto é,

$$\theta(\mu_1(p, P)) = \mu_2(\theta(p), P),$$

para todo $p \in C_1$ e $P \in E$.

A classe que contém E (afinal, E é um *twist* de si mesma!) é a **classe trivial**. A seguinte proposição mostra que saber quais espaços homogêneos para E são triviais está relacionado ao problema de determinar pontos racionais em curvas algébricas:

Proposição 4.1.7. Seja C um espaço homogêneo para E definido sobre K . Então, C está na classe trivial se, e somente se, $C(K)$ é não-vazio.

Prova. Por um lado, seja $\theta: E \rightarrow C$ um isomorfismo. Então, $\theta(O) \in C(K)$. Por outro lado, se $p_0 \in C(K)$, basta considerar o morfismo $\theta(P) = p_0 + P$ da Proposição 4.1.3. ■

As “subtrações” de espaços homogêneos equivalentes estão relacionadas:

Proposição 4.1.8. Se $\theta: C_1 \rightarrow C_2$ é uma equivalência de espaços homogêneos para E definidos sobre K , então, para todo $p, q \in C_1$,

$$\theta(q) - \theta(p) = q - p.$$

Definição 4.1.9. O conjunto das classes de equivalência dos espaços homogêneos para E é o **grupo de Weil–Châtelet** de E , denotado $\text{WC}(E)$.^[152]

O seguinte teorema mostra que $\text{WC}(E)$ é, de fato, um grupo:

Teorema 4.1.10. Existe uma bijeção $\text{WC}(E) \rightarrow H^1(\text{Gal}(\bar{K}/K), E)$ definida da seguinte forma: dada uma classe $[C] \in \text{WC}(E)$, tome um representante C e um ponto $p_0 \in C$. A bijeção leva $[C]$ em $[\sigma \mapsto p_0^\sigma - p_0]$.

Prova. O mapa está bem definido: o 1-cociclo $\sigma \mapsto p_0^\sigma - p_0$ é contínuo. Resta mostrar que o mapa $\text{WC}(E) \rightarrow H^1(\text{Gal}(\bar{K}/K), E)$ independente do representante de $[C]$ escolhido. Sejam

^[152]Quando necessário, destacaremos o corpo K sobre o qual a curva elíptica E é considerada para a definição do grupo de Weil–Châtelet por $\text{WC}(E/K)$.

$\theta: C \xrightarrow{\sim} C'$ dois representantes de $[C]$ e tome $p'_0 \in C'$. Pela Proposição 4.1.8, para cada $\sigma \in \text{Gal}(\bar{K}/K)$,^[153]

$$\begin{aligned} p_0^\sigma - p_0 &= \theta(p_0^\sigma) - \theta(p_0) \\ &= (p'_0)^\sigma - p'_0 + \underbrace{((\theta(p_0) - p'_0)^\sigma - (\theta(p_0) - p'_0))}_{\in B^1(\text{Gal}(\bar{K}/K), E)}. \end{aligned}$$

Portanto, o mapa está bem-definido.

Injetividade: sejam (C_1, p_1) e (C_2, p_2) tais que

$$[\sigma \mapsto p_1^\sigma - p_1] = [\sigma \mapsto p_2^\sigma - p_2],$$

ou seja, tais 1-cociclos diferem por um 1-cobordo gerado por certo $P_0 \in E$:

$$p_1^\sigma - p_1 = p_2^\sigma - p_2 + (P_0^\sigma - P_0) \quad \forall \sigma \in \text{Gal}(\bar{K}/K).$$

Deste modo, fica claro que o mapa

$$\begin{aligned} \theta: C_1 &\rightarrow C_2 \\ p &\mapsto p_2 - (p - p_1) + P_0 \end{aligned}$$

é um K -isomorfismo.

Sobrejetividade: seja $[\xi] \in H^1(\text{Gal}(\bar{K}/K), E)$. Podemos ver E como um subgrupo abeliano de $\text{Aut}(E)$ ^[154], associando a cada $P_0 \in E$ a translação $T_{P_0}: P \mapsto P + P_0$. Logo, $[\xi]$ pode ser visto dentro de $H^1(\text{Gal}(\bar{K}/K), \text{Aut}(E))$, isto é, $[\xi] = [\sigma \mapsto T_{-\xi(\sigma)}]$ ^[155]. Pelo Teorema 1.2.12, $[\xi]$ corresponde a um *twist* $\phi: C \rightarrow E$ de E , de modo que

$$T_{-\xi(\sigma)} = \phi^\sigma \circ \phi^{-1}, \quad \forall \sigma \in \text{Gal}(\bar{K}/K).$$

Colocaremos em C estrutura adequada para que esta se torne um espaço homogêneo para E , e que seja tal que sua classe em $\text{WC}(E)$ corresponda a $[\xi]$. Seja $\mu: C \times E \rightarrow C$ dado por

$$\mu(p, P) = \phi^{-1}(\phi(p) + P).$$

Segue das propriedades anteriores que μ é uma ação simplesmente transitiva e que $\mu(p, P)^\sigma = \mu(p^\sigma, P^\sigma)$, donde é um morfismo definido sobre K . Logo, (C, μ) é um espaço homogêneo para E .

^[153]Note que $\theta(p)^\sigma = \theta(p^\sigma)$, para todo $\sigma \in \text{Gal}(\bar{K}/K)$

^[154]Lembrando que $\text{Aut}(E)$ denota os automorfismos de E como curva algébrica, que não necessariamente são isogenias!

^[155]Observe que $-\xi(\sigma) \in E$. A escolha do sinal será justificada adiante.

Agora, mostraremos que $[C]$ corresponde a $[\xi]$. Seja $p_0 = \phi^{-1}(O)$. Então,

$$\begin{aligned} p_0^\sigma - p_0 &= (\phi^\sigma)^{-1}(O) - \phi^{-1}(O) \\ &= \phi^{-1} \circ T_{-\xi(\sigma)}^{-1}(O) - \phi^{-1}(O) \\ &= \phi^{-1}(O + \xi(\sigma)) - \phi^{-1}(O) \\ &\stackrel{4.1.8}{=} O + \xi(\sigma) - O = \xi(\sigma). \end{aligned}$$

Logo, o mapa $\text{WC}(E) \rightarrow H^1(\text{Gal}(\bar{K}/K), E)$ descrito é uma bijeção. ■

Agora, assumamos que $K = \mathbb{K}$ é um corpo de números. Mostraremos que o grupo de Weil–Châtelet é um subgrupo de torção, isto é, todo elemento tem ordem finita. Antes, precisamos de mais alguns conceitos e resultados auxiliares.

Definição 4.1.11. Seja $[\xi] \in H^1(\text{Gal}(\bar{\mathbb{K}}/\mathbb{K}), E)$. Dizemos que uma extensão $L/\mathbb{K}$ **cinde** $[\xi]$ se $\text{Res}([\xi]) = 0$, onde $\text{Res}: H^1(\text{Gal}(\bar{\mathbb{K}}/\mathbb{K}), E) \rightarrow H^1(\text{Gal}(\bar{\mathbb{K}}/L), E)$ é o mapa de restrição induzido pela inclusão $\mathbb{K} \hookrightarrow L$.

Lema 4.1.12. Seja $[\xi] \in H^1(\text{Gal}(\bar{\mathbb{K}}/\mathbb{K}), E)$. Então, existe uma extensão $L/\mathbb{K}$ de Galois finita que cinde $[\xi]$.

Prova. Seja $[\xi] = \sigma \mapsto p_0^\sigma - p_0$, onde C é um espaço homogêneo de E e $p_0 \in C$. Como C é um *twist* de E , existe uma extensão de Galois finita $L/\mathbb{K}$ sobre a qual E e C são isomorfos^[156]. Nesse caso, como C está na classe trivial, $\text{Res}([\xi]) \in H^1(\text{Gal}(\bar{\mathbb{K}}/L), E)$ está na classe de $\sigma \mapsto O^\sigma - O = 0$, donde L cinde $[\xi]$. ■

Teorema 4.1.13 (Lang–Tate). O grupo $\text{WC}(E)$ é de torção.

Prova. Seja $[C] \in \text{WC}(E)$ e considere a classe $[\xi] \in H^1(\text{Gal}(\bar{\mathbb{K}}/\mathbb{K}), E)$ correspondente. Pelo Lema 4.1.12, existe uma extensão de Galois $L/\mathbb{K}$ finita que cinde $[\xi]$. Logo, pela Proposição 1.2.11, $\text{Cores} \circ \text{Res}([\xi]) = \text{Cores}(0) = 0 = [L : \mathbb{K}][\xi]$. Assim, $[\xi]$, e portanto $[C]$, é de torção. ■

4.2 Sequências de Kummer

Daqui até o resto do capítulo, $m \geq 2$ é um inteiro, $\mathbb{K}$ é um corpo de números e $G = \text{Gal}(\bar{\mathbb{K}}/\mathbb{K})$. Considere a sequência exata de G -módulos

$$0 \longrightarrow E[m] \longrightarrow E(\bar{\mathbb{K}}) \xrightarrow{[m]} E(\bar{\mathbb{K}}) \longrightarrow 0.$$

Pela Proposição 1.2.9, temos uma sequência exata longa

^[156]Recordando a prova da Proposição 2.1.12, basta adicionar o u da mudança de coordenadas $(x, y) = (u^2x', u^3y')$ e, se necessário, tomar o fecho normal.

$$\begin{array}{ccccccc}
0 & \longrightarrow & E(\mathbb{K})[m] & \longrightarrow & E(\mathbb{K}) & \xrightarrow{[m]} & E(\mathbb{K}) \\
& & & & \searrow & & \uparrow \\
& & & & & \delta & \\
& & \searrow & & \longrightarrow & \xrightarrow{[m]} & \longrightarrow \\
& & H^1(G, E[m]) & \longrightarrow & H^1(G, E(\overline{\mathbb{K}})) & \longrightarrow & H^1(G, E(\overline{\mathbb{K}})).
\end{array}$$

Desta sequência, extraímos a **sequência exata de Kummer**^[157]:

$$0 \longrightarrow \frac{E(\mathbb{K})}{mE(\mathbb{K})} \xrightarrow{\delta} H^1(G, E[m]) \longrightarrow H^1(G, E)[m] \longrightarrow 0,$$

onde δ é, conforme a Proposição 1.2.9, dado da seguinte forma: dado $P \in E(\mathbb{K})$, tome qualquer $Q \in E(\overline{\mathbb{K}})$ tal que $[m](Q) = P$. Então, $\delta(P)$ é a classe de equivalência do 1-cociclo

$$\begin{aligned}
\xi : G &\rightarrow E[m] \\
\sigma &\mapsto Q^\sigma - Q.
\end{aligned}$$

Observação 4.2.1. O Teorema de Mordell–Weil (Teorema 3.1.1) nos motiva a estudar o grupo $E(\mathbb{K})/mE(\mathbb{K})$ ou, equivalentemente, a sua imagem em $H^1(G, E[m])$, que é o núcleo do mapa $H^1(G, E[m]) \rightarrow H^1(G, E)[m]$. Pelo Teorema 4.1.10, $H^1(G, E)[m] \cong \text{WC}(E)[m]$. Voltaremos a estas observações na seção seguinte.

Definição 4.2.2. Suponha que todos os pontos de m -torção de E são racionais sobre $\mathbb{K}$. O **pareamento de Kummer** é o mapa $\kappa : E(\mathbb{K}) \times G \rightarrow E[m]$ definido por $\kappa(P, \sigma) = Q^\sigma - Q$, onde $Q \in E(\overline{\mathbb{K}})$ é qualquer ponto tal que $[m](Q) = P$.

Proposição 4.2.3. O pareamento de Kummer é bilinear. Além disso, o núcleo de κ à esquerda é $mE(\mathbb{K})$ e o núcleo de κ à direita é $\text{Gal}(\overline{\mathbb{K}}/\mathbb{L})$, onde $\mathbb{L} = \mathbb{K}([m]^{-1}E(\mathbb{K}))$ é o menor corpo sobre o qual todo $Q \in E(\overline{\mathbb{K}})$ tal que $[m](Q) \in E(\mathbb{K})$ é racional^[158].

Prova. Como $E[m] \subseteq E(\mathbb{K})$, $H^1(G, E[m]) = \text{Hom}(G, E[m])$, donde temos um mapa injetor $E(\mathbb{K})/mE(\mathbb{K}) \hookrightarrow \text{Hom}(G, E[m])$ dado por $P \mapsto \kappa(P, \cdot)$. Logo, κ é bilinear.

Determinemos o núcleo de κ à esquerda, isto é, o conjunto dos P tais que $\kappa(P, \sigma) = O$ para todo $\sigma \in G$. Seja P nessas condições e escolha $Q \in E(\overline{\mathbb{K}})$ tal que $[m](Q) = P$. Temos que $\kappa(P, \sigma) = O$ se, e somente se, $Q^\sigma = Q$ para todo σ , isto é, Q é racional sobre $\mathbb{K}$ e $P \in mE(\mathbb{K})$. A recíproca é trivial.

Seja $P \in E$ e tome Q como acima. Note que Q é racional sobre $\mathbb{L}$, pela definição deste corpo. Logo, $\kappa(P, \sigma) = O$, para todo $\sigma \in \text{Gal}(\overline{\mathbb{K}}/\mathbb{L})$. Reciprocamente, se $\sigma \in G$ é tal que $\kappa(P, \sigma) = O$ para todo $P \in E(\mathbb{K})$, então, para todo $Q \in E(\overline{\mathbb{K}})$ tal que $[m](Q) \in E(\mathbb{K})$,

$$O = \kappa([m](Q), \sigma) = Q^\sigma - Q \implies Q^\sigma = Q.$$

^[157]Em analogia às curvas elípticas, denotamos por $A[m]$ o conjunto dos pontos de m -torção de um grupo A .

^[158]Note que $\mathbb{L}$ é, portanto, o compósito dos $\mathbb{K}(Q)$, *i.e.*, o menor corpo sobre o qual Q é racional, para todo Q nestas condições.

Logo, σ fixa $\mathbb{K}(Q)$, o menor corpo sobre o qual cada Q é racional, e portanto fixa o compósito de tais corpos, que é $\mathbb{L}$, donde $\sigma \in \text{Gal}(\overline{\mathbb{K}}/\mathbb{L})$. ■

Corolário 4.2.4. O pareamento de Kummer induz um pareamento perfeito^[159]

$$\bar{\kappa}: E(\mathbb{K})/mE(\mathbb{K}) \times \text{Gal}(\mathbb{L}/\mathbb{K}) \rightarrow E[m].$$

Prova. Pela Proposição 4.2.3, $\text{Gal}(\overline{\mathbb{K}}/\mathbb{L})$ é o núcleo do morfismo $G \rightarrow \text{Hom}(E(\mathbb{K}), E[m])$ dado por $\sigma \mapsto \kappa(\cdot, \sigma)$, sendo, portanto, um subgrupo normal de G e $\text{Gal}(\mathbb{L}/\mathbb{K}) \cong G/\text{Gal}(\overline{\mathbb{K}}/\mathbb{L})$. Logo, os núcleos à esquerda e à direita do pareamento induzido $\bar{\kappa}$ são triviais, donde κ é perfeito. ■

4.3 Grupos de Selmer e grupos de Tate–Shafarevich

Recorde a sequência exata de Kummer:

$$0 \longrightarrow \frac{E(\mathbb{K})}{mE(\mathbb{K})} \xrightarrow{\delta} H^1(G, E[m]) \longrightarrow \underbrace{H^1(G, E)[m]}_{\cong \text{WC}(E/\mathbb{K})} \longrightarrow 0.$$

Como comentamos na seção anterior (Observação 4.2.1), o Teorema de Mordell–Weil nos motiva a estudar o núcleo do mapa $H^1(G, E[m]) \rightarrow \text{WC}(E/\mathbb{K})$. Vimos também que determinar a classe trivial de $\text{WC}(E/\mathbb{K})$ está relacionado com o problema de encontrar pontos $\mathbb{K}$ -racionais em curvas elípticas (os *twists* de E), que é um problema difícil, em geral. Muito mais fácil é determinar pontos racionais de uma curva elíptica E sobre as extensões completas $\mathbb{K}_v$ de $\mathbb{K}$, pois reduzimos o problema a buscar pontos racionais sobre um corpo finito^[160]:

Proposição 4.3.1. Seja v um lugar não-arquimediano de $\mathbb{K}$. Se $\tilde{E}(k_v) \neq \emptyset$, então $E(\mathbb{K}_v) \neq \emptyset$.

Prova. Seja $E_0(\mathbb{K}_v)$ o subconjunto dos pontos de $E(\mathbb{K}_v)$ que têm redução não-singular. Se $\tilde{E}(k_v) \neq \emptyset$, então $\tilde{E}$ possui algum ponto k_v -racional não-singular^[161]. Logo, é suficiente mostrar que o mapa de redução módulo v restrito a $E_0(\mathbb{K}_v)$ é sobrejetor.

Seja $E: f(x, y) = 0$ um modelo v -integral e tome $\tilde{P} = (\alpha, \beta) \in \tilde{E}(k_v)$ não-singular. Então, $\tilde{P}$ não anula alguma das derivadas de $\tilde{f}$, digamos $\frac{\partial \tilde{f}}{\partial y}(\tilde{P}) \neq 0$. Tome $x_0 \in \mathcal{O}_v$ tal que $x_0 \equiv \alpha$

^[159]Note que um pareamento $e: M \times N \rightarrow L$ pode ser visto como um mapa linear $\Phi: M \rightarrow \text{Hom}(N, L)$, fazendo $\Phi(m)(n) = e(m, n)$. Neste caso, dizemos que e é um **pareamento perfeito** se Φ é um isomorfismo. Equivalentemente, e é perfeito se seus núcleos à esquerda e à direita são triviais.

^[160] $k_v \doteq \mathcal{O}_v/\mathfrak{m}_v$ é o corpo residual de v , que é uma extensão finita de $\mathbb{F}_p$, onde $(p) = \mathfrak{p}_v \cap \mathbb{Z}$, sendo $\mathfrak{p}_v$ o ideal primo de $\mathcal{O}_{\mathbb{K}}$ correspondente a v .

^[161]Isto é claro se a redução é boa. Se a redução é má, basta mostrar que $\tilde{E}(k_v)$ tem mais de um ponto, já que, pelo Teorema de Bézout (1.1.1), no máximo um ponto de $\tilde{E}$ é singular. A maioria dos casos está coberta pela Proposição 2.1.8 (para o caso em que a cúbica é nodal e as tangentes não estão definidas sobre k_v , use também o Teorema 90 de Hilbert (LANG, 2002, p. 288, Teorema 6.1)). Para o caso restante, em que $\tilde{E}: x^2 = (y - \alpha x)^2$ é cuspidal, $\text{car}(k_v) = 2$ e $\alpha \notin k_v$, basta notar que, para todo $t \in k_v$, $(t^2 + \alpha^2, t(t^2 + \alpha^2))$ é um ponto em $\tilde{E}(k_v)$.

mod $\mathfrak{m}_v$. A equação $f(x_0, y)$ tem raiz simples em $y = \beta$, donde, pelo Lema de Hensel, podemos tomar $y_0 \in \mathcal{O}_v$ tal que $y_0 \equiv \beta \pmod{\mathfrak{m}_v}$. Logo, (x_0, y_0) está na pré-imagem de $\tilde{P}$, donde o mapa é sobrejetor^[162]. ■

Isto nos motiva a estudar versões “locais” da sequência de Kummer para estudar a versão “global”^[164]. Seja v um lugar (qualquer) de $\mathbb{K}$ e escolha uma extensão de v para $\overline{\mathbb{K}}$. Na versão local, $\mathbb{K}_v$ substitui $\mathbb{K}$, $\overline{\mathbb{K}}_v$ substitui $\overline{\mathbb{K}}$ (note que a escolha de v determina o mergulho) e trocamos G pelo grupo de decomposição^[165] $D_v = \{\sigma \in G; v \circ \sigma = v\}$, obtendo a sequência exata

$$0 \longrightarrow \frac{E(\mathbb{K}_v)}{mE(\mathbb{K}_v)} \xrightarrow{\delta} H^1(D_v, E[m]) \longrightarrow WC(E/\mathbb{K}_v)[m] \longrightarrow 0.$$

Combinando a sequência exata global com as versões locais, obtemos o seguinte diagrama comutativo:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \frac{E(\mathbb{K})}{mE(\mathbb{K})} & \xrightarrow{\delta} & H^1(G, E[m]) & \longrightarrow & WC(E/\mathbb{K})[m] \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_{v \in \mathcal{S}_{\mathbb{K}}} \frac{E(\mathbb{K}_v)}{mE(\mathbb{K}_v)} & \xrightarrow{\delta} & \prod_{v \in \mathcal{S}_{\mathbb{K}}} H^1(D_v, E[m]) & \longrightarrow & \prod_{v \in \mathcal{S}_{\mathbb{K}}} WC(E/\mathbb{K}_v)[m] \longrightarrow 0. \end{array}$$

Deste diagrama, extraímos dois grupos que serão úteis para estudá-lo:

Definição 4.3.2. O m -grupo de Selmer de E é definido por

$$\text{Sel}_m(E) = \ker \left(H^1(G, E[m]) \rightarrow \prod_{v \in \mathcal{S}_{\mathbb{K}}} WC(E/\mathbb{K}_v) \right).$$

Definição 4.3.3. O grupo de Tate–Shafarevich de E é definido por^[166]

$$\text{III}(E) = \ker \left(WC(E/\mathbb{K}) \rightarrow \prod_{v \in \mathcal{S}_{\mathbb{K}}} WC(E/\mathbb{K}_v) \right).$$

^[162]Se $\tilde{P}$ fosse singular, poderia ocorrer que $\tilde{P}$ é ou não a redução módulo v de um ponto de E . Considere a curva elíptica $E: y^2 = x^3 + p$ sobre $\mathbb{Q}_p$ (é fácil checar que esta, e as próximas equações de Weierstrass mencionadas, estão na forma p -integral). Sua redução módulo p é má (aditiva) e o ponto singular $(0, 0) \in \tilde{E}$ não se levanta para um ponto em E . Por outro lado, considere a curva elíptica $E: y^2 = x^3 + p^3$ sobre $\mathbb{Q}_p$. O ponto singular $(0, 0)$, desta vez, pode ser levantado para $(0, -p)$ ^[163].

^[163]Para um exemplo usando o Lema de Hensel, considere a curva elíptica $E: y^2 = x^3 + p^2$ sobre $\mathbb{Q}_p$, com $p = 23$. Note que 16 é uma raiz simples de $x^3 - 2$ módulo p . Pelo Lema de Hensel, existe $b \in \mathbb{Z}_p$ tal que $b^3 = p + 2$, donde $(0, 0) \in \tilde{E}$ se levanta para $(pb, p^2 + p)$.

^[164]Esta nomenclatura não é por acaso: corpos de números são exemplos de **corpos globais** (os outros exemplos sendo, por definição, os corpos de funções de curvas sobre corpos finitos - com os quais os corpos de números têm muitas similaridades (POONEN, 2006, Seção 2.6)) e seus completamentos com relação a valorizações discretas são exemplos de **corpos locais** (TENGAN, 2008).

^[165]Note que, se v é não-arquimediano, D_v coincide com $D_{\mathfrak{p}_v}$, onde $\mathfrak{p}_v$ é o primo de $\mathcal{O}_{\mathbb{K}}$ que corresponde a v .

^[166]O símbolo III é a letra cirílica *sha*, a inicial do nome de Shafarevich em sua grafia original em russo.

Observação 4.3.4. As definições acima independem da escolha da extensão de v para $\overline{\mathbb{K}}$, pois, determinar se um elemento de $WC(E/\mathbb{K})$ se torna trivial em $WC(E/\mathbb{K}_v)$ é equivalente a checar se uma curva definida sobre $\mathbb{K}$ tem algum ponto $\mathbb{K}_v$ -racional, e isto claramente não é influenciado pela escolha da extensão de v que fizemos para obter a versão local da sequência de Kummer.

Observação 4.3.5. Essa ideia de transitar entre o global e o local é conhecida como **princípio de Hasse**, que essencialmente diz que é possível extrair propriedades de um objeto global a partir de suas versões locais. Neste caso, se $E(\mathbb{K}_v)$ é não-vazio para todo v , então $E(\mathbb{K})$ é não-vazio. No entanto, este princípio não é infalível: para um contraexemplo, ver [Aitken e Lemmermeyer \(2011\)](#), p. 16 (e para muitos, veja [Bhargava \(2014\)](#)!). Para mais sobre o princípio de Hasse e essa transição entre global e local, veja [Mazur \(1993\)](#).

O grupo de Tate–Shafarevich de uma curva elíptica, *grosso modo*, mede a falibilidade do princípio de Hasse para os espaços homogêneos de E : de fato, um espaço homogêneo de E não satisfaz o princípio de Hasse se, e somente se, corresponde a um elemento não-trivial de $III(E)$.

Agora, vejamos como os grupos definidos acima se relacionam.

Proposição 4.3.6 (*m*-Descida). Temos uma sequência exata

$$0 \longrightarrow E(\mathbb{K})/mE(\mathbb{K}) \longrightarrow \text{Sel}_m(E) \longrightarrow III(E)[m] \longrightarrow 0$$

(isto é imediato das definições e do diagrama comutativo da qual originam).

Como o Teorema fraco de Mordell–Weil foi o que nos motivou a chegar aqui, poderíamos tentar verificar se a imagem de $E(\mathbb{K})/mE(\mathbb{K})$ em $\text{Sel}_m(E)$ é finita.^[167] Na verdade, podemos fazer mais do que isto:

Proposição 4.3.7. Para todo $m \geq 2$, o m -grupo de Selmer $\text{Sel}_m(E)$ é finito.

A prova deste resultado será feita na próxima subseção.

Como consequência da finitude dos m -grupos de Selmer, obtemos o Teorema fraco de Mordell–Weil (Teorema 3.1.11):

Corolário 4.3.8 (Mordell–Weil). Para todo $m \geq 2$, $E(\mathbb{K})/mE(\mathbb{K})$ é finito.

4.3.1 Finitude dos grupos de Selmer

Antes de provar a finitude dos grupos de Selmer, elencaremos diversos conceitos e resultados que serão necessários para a demonstração.

^[167]Aliás, o nome *m*-descida faz referência ao Teorema da Descida Infinita (Teorema 3.1.6).

Proposição 4.3.9. Seja v um lugar não-arquimediano de $\mathbb{K}$ em que E tem boa redução e $v(m) = 0$, isto é, $\text{mdc}(m, \text{char}(k_v)) = 1$. Então, $\ker(\sim)$ não possui pontos de ordem m . Em particular, a restrição $E(\mathbb{K}_v)[m] \rightarrow \tilde{E}(k_v)$ é injetora.

Seja $E_1(\mathbb{K}) \doteq \ker(\sim)$. *Grosso modo*, mostraremos que $E_1(\mathbb{K})$ é isomorfo a um grupo proveniente de um *grupo formal* e, assim, aplicar a Proposição 4.3.11 a seguir. Os detalhes dos passos da demonstração deste resultado, que descreveremos sucintamente a seguir, podem ser encontrados no Capítulo IV de Silverman (2009), nas páginas indicadas.

Definição 4.3.10. Seja R um anel. Um **grupo formal** sobre R é uma série formal^[168] $F(x, y) \in R[[x, y]]$ tal que

- $F(x, y) = x + y + \underbrace{\quad \cdots \quad}_{\text{termos de grau } \geq 2}$;
- $F(x, F(y, z)) = F(F(x, y), z)$ (“associatividade”);
- $F(x, y) = F(y, x)$ (“comutatividade”);
- $F(0, y) = y$ e $F(x, 0) = x$ (“elemento neutro”);
- Existe único $i(t) \in R[[t]]$ tal que $F(t, i(t)) = 0$ (“inverso”).

Neste caso, denotamos o grupo formal por $\mathcal{F}$.

Grupos formais são “grupos sem elementos”. No entanto, podem ser usados para criar grupos de verdade: seja K um corpo completo com relação a uma valorização discreta v e $\mathcal{F}$ um grupo formal definido sobre $\mathcal{O}_v$. Então, $\mathfrak{m}_v$ com as operações

$$x + y = F(x, y) \quad \text{e} \quad -x = i(x)$$

é um grupo, denotado por $\mathcal{F}(\mathfrak{m}_v)$ ^[169].

Proposição 4.3.11. Seja $p = \text{char}(k_v)$. Então, todo elemento de torção de $\mathcal{F}(\mathfrak{m}_v)$ tem ordem p^n para algum n (*ibid.*, p. 124).

Prova. Seja $m > 1$ tal que $\text{mdc}(p, m) = 1$ e considere o mapa de multiplicação por m definido por

$$[m](T) = \underbrace{F(F(\dots(F(T, T))\dots))}_{m-1}.$$

^[168]Isto é, uma série para com que não nos importamos, *a priori*, com convergência.

^[169]As operações são fechadas pois, como K é completo, as séries convergem em $\mathfrak{m}_v$ (veja cada série como uma série em seus termos homogêneos e considere a sequência de suas somas parciais. Use o Teorema 1.4.12 para escrever x e y em termos de um parâmetro local e verifique que a sequência das somas parciais é Cauchy usando a propriedade ultramétrica de $|\cdot|_v$ para mostrar que, para todo n , as diferenças entre os termos da sequência eventualmente caem em $\mathfrak{m}_v^n$, ou seja, tendem a zero. Pela completude de K , a sequência converge. O limite está em $\mathfrak{m}_v$ porque este é um fechado).

Note que $f(T) \doteq [m](T) = mT + \underbrace{\dots}_{\text{termos de grau } \geq 2}$. Como $m \in \mathcal{O}_v^\times$, existe $g(T)$ tal que $f(g(T)) = g(f(T)) = T$. Logo, $[m]$ induz um automorfismo em $\mathcal{F}(\mathfrak{m}_v)$, donde $[m](x) = 0 \iff x = 0$. Logo, m não pode ser a ordem de um elemento de torção não-trivial. ■

Esboço da prova da Proposição 4.3.9. Começamos definindo o grupo formal associado a E . A ideia é investigar a soma de E perto de O . Para isto, começamos trocando as coordenadas, fazendo

$$z = -\frac{x}{y} \quad \text{e} \quad w = -\frac{1}{y},$$

de modo que O passa a ser a origem do plano afim. Usando a equação de Weierstrass de E , obtemos uma relação entre z e w :

$$w = z^3(1 + A_1z + A_2z^2 + \dots), \quad \text{com } A_i \in \mathbb{Z}[a_1, \dots, a_6]. \quad [170]$$

Retornando às coordenadas originais, também podemos expressar x e y em termos de z :

$$x(z) = \frac{1}{z^2} + \dots \quad \text{e} \quad y(z) = -\frac{1}{z^3} + \dots$$

(*ibid.*, p. 118). Para definir o grupo formal, imitaremos a construção da soma de uma curva elíptica: tomamos o terceiro ponto da curva na reta definida pelas parcelas e o invertemos. Sejam $(z_1, w_1(z_1))$ e $(z_2, w_2(z_2))$ dois pontos e denote por $(z_3(z_1, z_2), w_3(z_3))$ o terceiro ponto de E na reta definida por eles. Assim como o inverso de (x, y) é $(x, -y - a_1x - a_3)$, a primeira coordenada de $-(z, w(z))$ é

$$i(z) \doteq \frac{x(z)}{y(z) + a_1x(z) + a_3}.$$

Deste modo, o grupo formal associado a E é definido por

$$\widehat{E}(z_1, z_2) = i(z_3(z_1, z_2)).$$

Agora, considere o grupo $\widehat{E}(\mathfrak{m}_v)$. O mapa

$$\begin{aligned} \widehat{E}(\mathfrak{m}_v) &\rightarrow E(\mathbb{K}_v) \\ z &\mapsto (x(z), y(z)) \end{aligned}$$

é um morfismo de grupos e é injetor, pois possui inversa $(x, y) \mapsto -\frac{x}{y}$. Além disso, esta inversa também é um morfismo de grupos injetor, donde o mapa acima é um isomorfismo (*ibid.*, p. 191, Proposição 2.2). Logo, pela Proposição 4.3.11, $E_1(\mathbb{K})$ só possui pontos de ordem p^n para algum n , onde $p = \text{char}(k_v)$. Como $\text{mdc}(m, p) = 1$, $E_1(\mathbb{K})$ não possui pontos de ordem m . □

Proposição 4.3.12. Seja v um lugar não-arquimediano de $\mathbb{K}$ em que E tem boa redução. Então, $\widetilde{\cdot}: E(\mathbb{K}_v) \rightarrow \widetilde{E}(k_v)$ é um morfismo sobrejetor.

[170] A convergência de $w(z)$ usa o Lema de Hensel (*ibid.*, p. 116, Proposição IV.1.1)

Prova. Pela Proposição 4.3.1, já sabemos que este mapa é sobrejetor. Resta mostrar que a redução módulo v $E(\mathbb{K}_v) \rightarrow \tilde{E}(k_v)$ é um morfismo de grupos, mas isto é claro, já que a redução módulo v preserva colinearidade (ainda que dois pontos reduzam para o mesmo ponto) e multiplicidades de intersecção. ■

Proposição 4.3.13. Seja $S \subseteq \mathcal{S}_{\mathbb{K}}$ tal que $\mathcal{S}_{\mathbb{K}}^{\text{narq}} \subseteq S$ e $\mu \geq 2$. Seja $L/\mathbb{K}$ a extensão maximal satisfazendo as seguintes propriedades:

- $\text{Gal}(L/\mathbb{K})$ é abeliano e a ordem de cada elemento deste grupo divide μ (isto é, a extensão é abeliana de expoente μ);
- $L/\mathbb{K}$ é não-ramificada fora de S .

Então, $L/\mathbb{K}$ é uma extensão finita (SILVERMAN, 2009, p. 194, Proposição VII.1.6).

Definição 4.3.14. Seja M um G -módulo e $v \in \mathcal{S}_{\mathbb{K}}^{\text{narq}}$. Uma classe de co-homologia $[\xi] \in H^1(G, M)$ **não ramifica** em v se torna-se trivial quando restrita a $H^1(I_v, M)$, onde I_v denota o grupo de inércia de (o primo associado a) v .

Lema 4.3.15. Seja M um G -módulo abeliano finito e $S \subseteq \mathcal{S}_{\mathbb{K}}^{\text{narq}}$ finito. O conjunto

$$H^1(G, M; S) \doteq \{[\xi] \in H^1(G, M); [\xi] \text{ não ramifica em nenhum } v \notin S\}$$

é finito.

Prova. Como M é finito, é fixado por um subgrupo $H \leq G$ de índice finito. Logo, se mostrarmos o resultado para $\overline{\mathbb{K}}^H$ em vez de $\mathbb{K}$, que é uma extensão finita de $\mathbb{K}$, segue da sequência de Inflação-Restrição (Proposição 1.2.10) o resultado para $\mathbb{K}$. Assim, podemos supor que G age trivialmente sobre M , isto é, que os grupos de co-homologia são, na verdade, grupos de morfismos.

Seja μ o menor inteiro positivo tal que $\mu a = 0$ para todo $a \in M$ e seja $L/\mathbb{K}$ a extensão abeliana maximal de expoente μ e que não ramifica fora de S . Pela Proposição 4.3.13, $L/\mathbb{K}$ é finita, donde $\text{Hom}(\text{Gal}(L/\mathbb{K}), M; S)$, definido analogamente, também o é.

A sequência de Inflação-Restrição, neste caso, é dada por

$$0 \longrightarrow \text{Hom}(\text{Gal}(L/\mathbb{K}), M; S) \xrightarrow{\text{Inf}} \text{Hom}(G, M; S) \xrightarrow{\text{Res}} \text{Hom}(\text{Gal}(\overline{\mathbb{K}}/L), M; S).$$

Se mostrarmos que a imagem de Res é trivial, Inf será um isomorfismo e teremos o resultado. Seja $\phi \in \text{Hom}(G, M)$. Note que $\overline{\mathbb{K}}^{\ker(\phi)}$ é uma extensão abeliana de expoente μ não-ramificada fora de S . Logo, $\overline{\mathbb{K}}^{\ker(\phi)} \subseteq L \implies \text{Gal}(L/\mathbb{K}) \subseteq \ker(\phi) \implies \text{Res}(\phi) = 0$. ■

Enfim, estamos prontos para a prova da finitude dos grupos de Selmer:

Prova da Proposição 4.3.7. Seja $[\xi] \in \text{Sel}_m(E)$ e considere $S \subseteq \mathcal{S}_{\mathbb{K}}$ dado por^[171]

$$S = \mathcal{S}_{\mathbb{K}}^{\text{arq}} \cup \{v \in \mathcal{S}_{\mathbb{K}}^{\text{narq}}; v(m) \neq 0\} \cup \{v \in \mathcal{S}_{\mathbb{K}}^{\text{narq}}; E \text{ tem redução má em } v\}.$$

Seja $v \in S$. Como $[\xi]$ é trivial em $\text{WC}(E/\mathbb{K}_v)$, temos que, pelo Teorema 4.1.10, $[\xi] = [\sigma \mapsto P^\sigma - P] \in H^1(D_v, E(\overline{\mathbb{K}}_v))$ para algum $P \in E(\overline{\mathbb{K}}_v)$. Se $\sigma \in I_v = I_{\mathfrak{m}_v}$, então

$$P^\sigma \equiv P \pmod{\mathfrak{m}_v} \implies (P^\sigma - P)^\sim = \tilde{O}.$$

Além disso, pela própria definição de $[\xi]$, $P^\sigma - P \in E[m]$. Logo, $P^\sigma - P$ está no núcleo do mapa $E(\mathbb{K}_v)[m] \rightarrow \tilde{E}(k_v)$, donde, pela Proposição 4.3.9, $P^\sigma = P$. Logo, $[\xi]$ é trivial como elemento de $H^1(I_v, E)$, e, portanto, $[\xi]$ não ramifica fora do conjunto finito S . Pelo Lema 4.3.15, $\text{Sel}_m(E) \subseteq H^1(G, E[m]; S)$ é finito. ■

Assim, $\text{Sel}_m(E)$ é (pelo menos teoricamente) computável: o grupo finito $H^1(G, E[m]; S)$ é (teoricamente) computável e, para saber se um elemento $[\xi]$ dele cai no m -grupo de Selmer, observa-se $[\xi]$ como um elemento $[C]$ de $\text{WC}(E)$ e checka-se, para os finitos $v \in S$, se $C(\mathbb{K}_v) \neq \emptyset$. Pela Proposição 4.3.1, esta verificação pode ser feita em tempo finito (SILVERMAN, 2009, p. 334, Remark X.4.5).^[172]

4.3.2 Finitude do grupo de Tate–Shafarevich

Poderíamos nos perguntar se, assim como os grupos de Selmer, o grupo de Tate–Shafarevich de uma curva elíptica sobre $\mathbb{K}$ também é finito. Quanto a isto...

Conjectura 4.3.16 (Tate–Shafarevich). O grupo de Tate–Shafarevich $\text{III}(E)$ é finito.

Porém, no caso $\mathbb{K} = \mathbb{Q}$, há um resultado poderoso de Rubin (1991) e Kolyvagin (1988) que mostra que tanto a conjectura de Tate–Shafarevich quanto a conjectura de Birch e Swinnerton-Dyer são válidas para curvas elípticas com posto analítico 0 ou 1!

Teorema 4.3.17 (Kolyvagin–Rubin). Seja E uma curva elíptica sobre $\mathbb{Q}$. Se $r_{\text{an}}(E) \leq 1$, então $r_{\text{an}}(E) = r_{\text{alg}}(E)$ e $\text{III}(E)$ é finito.^[173]

^[171]Note que S é finito, pois o número de lugares arquimedianos depende do número de (finitos) mergulhos de $\mathbb{K}$ em $\mathbb{R}$ ou $\mathbb{C}$ (ver subseção 1.6.3) e que, para todo $a \in \mathbb{K}$, $v_p(a) \neq 0 \iff p$ faz parte da fatoração de (a) . Em particular, E tem redução má $\iff v(\Delta(E)) > 0$ em apenas um número finito de lugares.

^[172]Como aponta (POONEN, 2002), p. 7, Corolário 3, da finitude de $\text{Sel}_m(E)$, também temos que $E(\mathbb{K})/mE(\mathbb{K})$ e $\text{III}(E)[m]$ são finitos, mas não conseguimos computá-los a partir do m -grupo de Selmer pois não é possível saber, na prática, quanto de $\text{Sel}_m(E)$ vem de $E(\mathbb{K})/mE(\mathbb{K})$ e quanto de tal grupo se anula em $\text{III}(E)[m]$. Na p^∞ -descida, discutida adiante na seção 4.3.4, a situação é um pouco mais favorável que a da m -descida, pois, naquele caso, a sequência exata cinde (Proposição 4.3.36).

^[173]Se E tem redução multiplicativa não-*split* em pelo menos um primo ímpar ou redução multiplicativa *split* em dois primos ímpares, então vale a recíproca: $r_{\text{alg}}(E) = 1$ e $\#\text{III}(E) < \infty$ implica $r_{\text{an}}(E) = 1$ (SKINNER, 2014a, Teorema A').

Em particular, acrescentando à discussão da seção 3.3.1, se soubermos que $r_{\text{an}}(E) \leq 1$, o que é fácil de se verificar, obtemos o posto algébrico de E !^[174]

Por outro lado, para $r_{\text{an}}(E) > 1$, não se conhece nem sequer um exemplo em que a conjectura de Tate–Shafarevich é válida^[175]. Porém, curiosamente, sabe-se que, se tal grupo for finito, sua ordem será um quadrado perfeito!

Teorema 4.3.18 (Cassels). Seja E uma curva elíptica sobre $\mathbb{Q}$. Então, existe um pareamento alternado bilinear

$$\Gamma: \text{III}(E) \times \text{III}(E) \rightarrow \mathbb{Q}/\mathbb{Z},$$

cujos núcleos laterais são $\text{III}(E)_{\text{div}}$, o subgrupo dos elementos divisíveis (Definição 1.3.1). Se $\text{III}(E)$ for finito, então Γ é não-degenerado e $\#\text{III}(E)$ é um quadrado^[176]. (CASSELS, 1962).

O pareamento de Cassels se restringe a um pareamento não-degenerado em $\text{III}(E)_{\text{nd}} \doteq \text{III}(E)/\text{III}(E)_{\text{div}}$. Assim, como no teorema anterior, se este subgrupo for finito, sua ordem é um quadrado (na verdade, esperamos que, como o subgrupo divisível é infinito, $\text{III}(E)_{\text{div}} = 0$, e portanto $\text{III}(E) = \text{III}(E)_{\text{nd}}$). E mais pode ser dito sobre a estrutura deste grupo:

Teorema 4.3.19. Se $\text{III}(E)_{\text{nd}}$ é finito, então $\text{III}(E)_{\text{nd}} \cong T \oplus T$ para algum grupo abeliano finito T (POONEN; STOLL, 1999, p. 12, Corolário 9 (1)).

A conjectura forte de Birch e Swinnerton-Dyer relaciona a ordem de $\text{III}(E)$ com o coeficiente líder de $L(s, E)$, fornecendo uma possível maneira de calculá-la^[177] (mais detalhes no apêndice A.1). Por enquanto, como nem se sabe se $\text{III}(E)$ é sempre finito, também certamente não se conhecem maneiras de computá-lo em geral.

Como $\text{III}(E)$ é um subgrupo de $\text{WC}(E)$, que é de torção (Teorema 4.1.13),

$$\text{III}(E) = \bigcup_{m=1}^{\infty} \text{III}(E)[m].$$

Logo, computar as partes de torção, ou mesmo as partes p -primárias

$$\text{III}(E)[p^{\infty}] \doteq \bigcup_{m=1}^{\infty} \text{III}(E)[p^m]$$

pode ser a chave para computar o grupo todo, mas, também para estes casos, não há métodos que funcionem para qualquer curva elíptica. No entanto, este cenário já é mais favorável para

^[174]Parece pouco, mas a condição $r_{\text{an}}(E) \leq 1$ tende a ser satisfeita pela maioria, e, esperadamente, por quase todas, as curvas elípticas sobre $\mathbb{Q}$! Veja o capítulo 5 para mais detalhes.

^[175]Bertolini e Darmon (2007) se referem à dificuldade de se encontrar evidências para a validade da Conjectura BSD no caso $r_{\text{an}}(E) > 1$ como “o desafio último da conjectura BSD” (*op. cit.*, p. 9).

^[176]Veja, por exemplo, Davydov (2018), p. 12, para uma prova de que a existência de um pareamento alternado bilinear não-degenerado $\Gamma: G \times G \rightarrow H$ implica que a ordem de G , caso seja finito, é um quadrado.

^[177]A ordem prevista para $\text{III}(E)$ pela conjectura BSD forte é chamada **ordem analítica** de $\text{III}(E)$, em analogia aos postos, visto que o posto analítico de E é o posto (algébrico) previsto para E pela conjectura BSD.

verificações computacionais de casos particulares, fornecendo evidência para a conjecturada finitude de $\text{III}(E)$.

Observação 4.3.20. O pareamento de Cassels se restringe, tomando partes p -primárias, a um pareamento $\Gamma_p: \text{III}(E)[p^\infty] \times \text{III}(E)[p^\infty] \rightarrow (\mathbb{Q}/\mathbb{Z})[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$, que é não-degenerado se $\text{III}(E)[p^\infty]$ for finito (porque $\text{III}(E)[p^\infty]$ necessariamente seria trivial). Neste caso, a ordem da parte p -primária de $\text{III}(E)$ também seria um quadrado.

Na prática, queremos que o grupo de Tate–Shafarevich seja trivial - ou, pelo menos, que algum subgrupo de m -torção o seja - pois, neste caso, $E(\mathbb{Q})/mE(\mathbb{Q}) \cong \text{Sel}_m(E)$ e, dada a computabilidade de $\text{Sel}_m(E)$, temos uma maneira de acessar o posto algébrico de E ^[178].

4.3.3 A p -descida e o posto algébrico

Daqui em diante, $\mathbb{K} = \mathbb{Q}$ e p é um primo fixo. Considere a sequência exata de p -descida (Proposição 4.3.6)

$$0 \longrightarrow E(\mathbb{Q})/pE(\mathbb{Q}) \longrightarrow \text{Sel}_p(E) \longrightarrow \text{III}(E)[p] \longrightarrow 0.$$

Se $E(\mathbb{Q}) = \mathbb{Z}^{r_{\text{alg}}(E)} \oplus T$, temos que $E(\mathbb{Q})/pE(\mathbb{Q}) = \mathbb{F}_p^{r_{\text{alg}}(E)} \oplus T/pT$. Se a ordem de $x \in T$ não é uma potência de p , então $\bar{x} = \bar{0} \in T/pT$. Logo, T/pT só recebe contribuições da parte p -primária de E . Porém, pelo Teorema de Mazur (Teorema 3.1.2), $\dim_{\mathbb{F}_p}(T/pT) = 0$ para $p \geq 11$. Logo, a torção de $E(\mathbb{Q})$ só contribui nos casos pequenos ($p = 2, 3, 5$ ou 7).

Observe que $\#\text{Sel}_p(E) = \#E(\mathbb{Q})/pE(\mathbb{Q}) \cdot \#\text{III}(E)[p] = p^{s_p(E)}$, para algum $s_p(E) \in \mathbb{Z}_{\geq 0}$, que chamamos **p -posto de Selmer** de E . Este número se relaciona com o posto algébrico E da seguinte forma:

$$\begin{aligned} \dim_{\mathbb{F}_p}(\text{Sel}_p(E)) &= \dim_{\mathbb{F}_p}(E(\mathbb{Q})/pE(\mathbb{Q})) + \dim_{\mathbb{F}_p}(\text{III}(E)[p]) \\ s_p(E) &= r_{\text{alg}}(E) + \underbrace{\dim_{\mathbb{F}_p}(T/pT)}_{= 0 \text{ quase sempre}} + \dim_{\mathbb{F}_p}(\text{III}(E)[p]) \geq r_{\text{alg}}(E). \end{aligned}$$

Em vista da discussão sobre maneiras de computar o posto algébrico da seção 3.3.1, o p -posto de Selmer de E é essencialmente a única maneira de obter cotas superiores para o posto algébrico de E ^[179]. Observe também que a dificuldade em se determinar $\text{III}(E)[p]$ nos impede de usar a fórmula acima como mais uma maneira de calcular $r_{\text{alg}}(E)$.

^[178]Veja o artigo de [Stein e Wuthrich \(2013\)](#), onde se computa a parte p -primária de $\text{III}(E)$ para um grande número de curvas elípticas e, obtendo-se, em todos os casos, que tais subgrupos são triviais!

^[179]Conforme aponta B. Poonen em sua palestra “Heuristics for the arithmetic of elliptic curves” no ICM 2018 (<<https://www.youtube.com/watch?v=yxyz2K1UX9Y>>).

4.3.4 A p^∞ -descida e o posto algébrico

Podemos dar um passo além e considerar todas as sequências exatas de p^e -descida para todo $e \in \mathbb{N}$ de uma só vez, por meio do limite direto:

Definição 4.3.21. Seja $(I, \leq)$ um conjunto direcionado (ver nota [19]) e $\{A_i\}_{i \in I}$ uma família de grupos, tais que, dados $i, j \in I$, existem morfismos $\phi_{ij}: A_i \rightarrow A_j$ para todo $j \geq i$, de modo que $\phi_{ii} = id_{A_i}$ e que são compatíveis com composição, ou seja, se $k \geq j \geq i$, $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$. O **limite direto** da família $\{A_i\}$ é o conjunto^[180]

$$\varinjlim_{i \in I} A_i \doteq \bigsqcup_{i \in I} A_i / \sim,$$

onde $x_i \in A_i$ e $x_j \in A_j$ são equivalentes se, e somente se, existe $k \geq i, j$ tal que $\phi_{ik}(x_i) = \phi_{jk}(x_j)$ ^[181].

Em particular, se G é um grupo abeliano, $G[p^\infty] = \varinjlim_{e \in \mathbb{N}} G[p^e]$, onde $G[p^e]$ denota a p^e -torção de G ($e = \infty$ denota a parte p -primária) e ϕ_{ij} é a inclusão $G[p^i] \hookrightarrow G[p^j]$. Isto é, identificamos as várias cópias de um mesmo elemento que aparecem repetidas em cada $G[p^e]$.

Proposição 4.3.22. O limite direto é exato, isto é, se $(A_i, \phi_\bullet)$, $(B_i, \psi_\bullet)$, $(C_i, \omega_\bullet)$, com $i \in I$, são famílias nas condições da definição acima e as sequências

$$0 \longrightarrow A_i \xrightarrow{f_i} B_i \xrightarrow{g_i} C_i \longrightarrow 0$$

são exatas, então existe uma sequência exata

$$0 \longrightarrow \varinjlim_{i \in I} A_i \xrightarrow{f} \varinjlim_{i \in I} B_i \xrightarrow{g} \varinjlim_{i \in I} C_i \longrightarrow 0$$

(Stacks project authors, 2020, Parte 1, Capítulo 10, Seção 10.8, Lema 10.8.8).

Tomando o limite direto^[182] das sequências exatas de p^e -descida, obtemos a sequência exata de p^∞ -descida

$$0 \longrightarrow \varinjlim_{e \in \mathbb{N}} E(\mathbb{Q})/p^e E(\mathbb{Q}) \longrightarrow \varinjlim_{e \in \mathbb{N}} \text{Sel}_{p^e}(E) \longrightarrow \varinjlim_{e \in \mathbb{N}} \text{III}(E)[p^e] \longrightarrow 0,$$

^[180] $\bigsqcup_{i \in I} A_i \doteq \bigcup_{i \in I} A_i \times \{i\}$ denota a **união disjunta** dos A_i , isto é, colocamos em cada elemento uma “etiqueta” marcando de qual A_i ele veio. Logo, se um mesmo elemento aparece em dois A_i distintos, na união disjunta, estes elementos serão distintos.

^[181] Isto é, “em algum momento, x_i e x_j se tornam iguais”.

^[182] onde os mapas considerados são as inclusões.

Já vimos que o quarto termo desta sequência é o misterioso $\text{III}(E)[p^\infty]$. O segundo é

$$\lim_{e \in \mathbb{N}} E(\mathbb{Q})/p^e E(\mathbb{Q}) \stackrel{[183]}{\cong} \lim_{e \in \mathbb{N}} (E(\mathbb{Q}) \otimes (\mathbb{Q}/\mathbb{Z})[p^e]) \cong E(\mathbb{Q}) \otimes \lim_{e \in \mathbb{N}} (\mathbb{Q}/\mathbb{Z})[p^e] \cong E(\mathbb{Q}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$$

O terceiro termo é, por definição, o p^∞ -grupo de Selmer:

$$\text{Sel}_{p^\infty}(E) \doteq \lim_{e \in \mathbb{N}} \text{Sel}_{p^e}(E).$$

Assim, a sequência exata de p^∞ -descida pode ser escrita como^[184]

$$0 \longrightarrow E(\mathbb{Q}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \text{Sel}_{p^\infty}(E) \longrightarrow \text{III}(E)[p^\infty] \longrightarrow 0.$$

Agora, vamos explorar com mais detalhes a estrutura de $\text{Sel}_{p^\infty}(E)$.^[185]

Definição 4.3.23. Sejam X e Y dois espaços topológicos e $Z = \mathcal{C}(X, Y)$ o conjunto das funções contínuas de X para Y . A **topologia compacto-aberto** em Z é a menor topologia que contém os conjuntos da forma

$$(K, O) \doteq \{f \in Z; f(K) \subseteq O\},$$

onde $K \subseteq X$ é compacto e $O \subseteq Y$ é um aberto.

Definição 4.3.24. Seja M um $\mathbb{Z}_p$ -módulo localmente compacto. O **dual de Pontryagin** de M é o $\mathbb{Z}_p$ -módulo de morfismos contínuos $\text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, denotado por $\widehat{M}$, que é topológico com a topologia compacto-aberto^[186].

O $\mathbb{Z}_p$ -módulo $\widehat{M}$ também é localmente compacto (HEWITT; ROSS, 1979, p. 361, Teorema 23.15). Logo, faz sentido considerar o dual do dual:

Teorema 4.3.25 (Pontryagin-van Kampen). Seja M um $\mathbb{Z}_p$ -módulo localmente compacto. Então, $M \cong \widehat{\widehat{M}}$ (MORRIS, 1977, p. 84, Teorema 23).

^[183]O isomorfismo $E(\mathbb{Q})/p^e E(\mathbb{Q}) \rightarrow E(\mathbb{Q}) \otimes (\mathbb{Q}/\mathbb{Z})[p^e]$ é dado por $\bar{P} \mapsto P \otimes \frac{1}{p^e}$. Para informações sobre produtos tensoriais de $(\mathbb{Z}-)$ módulos, veja Lang (2002), p. 601, Capítulo 14.

^[184]Um artigo de Bhargava *et al.* (2013) trata da probabilidade de uma sequência exata curta de $\mathbb{Z}_p$ -módulos qualquer ser a sequência de p^∞ -descida de uma curva elíptica. Enuncia-se uma conjectura respeito desta probabilidade, cuja validade teria consequências incríveis, como a finitude das partes p -primárias de $\text{III}(E)$ de 100% das curvas elípticas, quando ordenadas por altura; a Conjectura de Goldfeld–Katz–Sarnak sobre o posto algébrico médio (Conjectura 5.1.19 – e, portanto, todas as suas notáveis consequências!) e, a partir de uma generalização do método utilizado, a Conjectura de Bhargava sobre o tamanho médio dos m -grupos de Selmer (Conjectura 5.3.8)! Veja o capítulo seguinte para uma discussão destas conjecturas mencionadas.

^[185]A seguir, assumiremos conceitos e resultados básicos de Álgebra Comutativa e Topologia, que podem ser consultados em Borges e Tengan (2015) e Atiyah e MacDonald (1969), Aurichi (2017) e McCarty (1988).

^[186]Onde $\mathbb{Q}_p/\mathbb{Z}_p$ possui a topologia quociente. Para mais detalhes sobre a topologia compacto-aberto, veja (MCCARTY, 1988, p. 166)

Observação 4.3.26. Um p -grupo abeliano G é um $\mathbb{Z}_p$ -módulo: como $g \in G$ tem ordem p^N para algum N , $\sum_{i=0}^{\infty} a_i p^i \cdot g = \sum_{i=0}^{N-1} a_i p^i \cdot g \in G$. Pelo mesmo motivo, um morfismo de p -grupos abelianos $\varphi: G \rightarrow H$ se estende para um morfismo de $\mathbb{Z}_p$ -módulos. Assim, dois p -grupos abelianos são isomorfos como grupos se, e somente se, são isomorfos como $\mathbb{Z}_p$ -módulos.

Logo, como todos os $\mathbb{Z}_p$ -módulos de que trataremos a seguir também são p -grupos abelianos, podemos trabalhar no contexto de grupos sempre que conveniente.

A seguir, veremos diversos exemplos (e resultados auxiliares exigidos por cada um) que serão úteis para a compreensão da estrutura de $\text{Sel}_{p^\infty}(E)$.

Exemplo 4.3.27. O dual de Pontryagin de $\mathbb{Z}_p$ é $\mathbb{Q}_p/\mathbb{Z}_p$.

Prova. Todo morfismo de $\mathbb{Z}_p$ -módulos $\phi: \mathbb{Z}_p \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ fica bem definido escolhendo-se $\phi(1)$. Para cada $z \in \mathbb{Q}_p/\mathbb{Z}_p$, denote por ϕ_z o morfismo definido por $\phi_z(1) = z$, que é contínuo. Logo, $f: \mathbb{Q}_p/\mathbb{Z}_p \rightarrow \widehat{\mathbb{Z}_p}$ dado por $z \mapsto \phi_z$ é um isomorfismo de $\mathbb{Z}_p$ -módulos. Resta mostrar que é contínuo.

Considere o mapa inverso $g: \widehat{\mathbb{Z}_p} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ dado por $\phi \mapsto \phi(1)$. Como grupos topológicos são homogêneos^[187], basta checar a continuidade em $0 \in \widehat{\mathbb{Z}_p}$. Seja $V \ni g(0) = 0$ uma vizinhança aberta. Então, $U = \{\phi \in \widehat{\mathbb{Z}_p}; \phi(1) \in V\}$ é uma vizinhança aberta de 0 em $\widehat{\mathbb{Z}_p}$, pela definição da topologia compacto-aberto. Como $g(U) \subseteq V$, temos que g é contínuo. ■

Note que $\mathbb{Z}_p$ (e qualquer bola fechada em $\mathbb{Q}_p$) é compacto e $\mathbb{Q}_p/\mathbb{Z}_p$, seu dual, é discreto. Na verdade, esta dualidade se estende para os outros $\mathbb{Z}_p$ -módulos de que tratamos aqui:

Lema 4.3.28. Se M é um $\mathbb{Z}_p$ -módulo localmente compacto discreto, $\widehat{M}$ é compacto. Reciprocamente, se M é compacto, $\widehat{M}$ é discreto (MORRIS, 1977, p. 50, Teorema 12).

Proposição 4.3.29. Sejam $M_1, \dots, M_n$ $\mathbb{Z}_p$ -módulos localmente compactos. Então,

$$(M_1 \oplus \dots \oplus M_n)^\wedge \cong \widehat{M_1} \oplus \dots \oplus \widehat{M_n}.$$

Prova. Considere o mapa

$$\Phi: (M_1 \oplus \dots \oplus M_n)^\wedge \rightarrow \widehat{M_1} \oplus \dots \oplus \widehat{M_n} \quad (4.1)$$

$$\phi \mapsto (\phi \circ \iota_1, \dots, \phi \circ \iota_n) \quad (4.2)$$

onde $\iota_i: M_i \hookrightarrow M_1 \oplus \dots \oplus M_n$ é a imersão dada por $m_i \mapsto (0, \dots, 0, \underbrace{m_i}_i, 0, \dots, 0)$, que é contínua.

É fácil ver que este mapa é um isomorfismo de $\mathbb{Z}_p$ -módulos. Compondo Φ com a projeção

^[187]Seja G um grupo topológico. Dados $g_1, g_2 \in G$, $g \mapsto g_2 - g_1 + g$ é um homeomorfismo que leva g_1 em g_2 .

$\Pi_i: \widehat{M}_1 \oplus \cdots \oplus \widehat{M}_n \rightarrow \widehat{M}_i$, obtemos o mapa $\phi \mapsto \phi \circ \iota_i$, que é contínuo. Logo, Φ é contínuo (AURICHI, 2017, p. 62, Teorema 3.2.4). ■

Exemplo 4.3.30. O dual de Pontryagin de um p -grupo abeliano finito G é isomorfo a G .

Prova. Um p -grupo abeliano finito é um $\mathbb{Z}_p$ -módulo (veja Observação 4.3.26), que é topológico com a topologia discreta. Como todo grupo abeliano finito é um produto de grupos cíclicos (por exemplo, pelo Teorema 4.3.34 a seguir), basta supormos que $G \cong \mathbb{Z}/p^n\mathbb{Z}$ é cíclico.

Note que, para todo $g \in G$, $p^n g = 0$. Logo, para qualquer $\phi \in \widehat{G}$, $p^n \phi(g) = 0$, donde $\widehat{G} = \text{Hom}_{\mathbb{Z}_p}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z})$. Como $\mathbb{Z}/p^n\mathbb{Z}$ é cíclico, basta escolher a imagem de $\bar{1}$, para o que temos p^n opções. Logo,

$$\widehat{G} = \text{Hom}_{\mathbb{Z}_p}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p^n\mathbb{Z} \cong G. \quad \blacksquare$$

A continuidade deste isomorfismo segue como no Exemplo 4.3.27.

Exemplo 4.3.31. Seja G um p -grupo abeliano tal que $G[p^e]$ é finito para todo $e \in \mathbb{N}$.

$$\widehat{G} = \text{Hom}_{\mathbb{Z}_p}(G, \mathbb{Q}_p/\mathbb{Z}_p) = \text{Hom}_{\mathbb{Z}_p}(\varprojlim_{e \in \mathbb{N}} G[p^e], \mathbb{Q}_p/\mathbb{Z}_p) \stackrel{[188]}{\cong} \varprojlim_{e \in \mathbb{N}} \text{Hom}_{\mathbb{Z}_p}(G[p^e], \mathbb{Q}_p/\mathbb{Z}_p) \cong \varprojlim_{e \in \mathbb{N}} G[p^e].$$

O grupo $\varprojlim_{e \in \mathbb{N}} G[p^e]$ é chamado **módulo de Tate p -ádico**^[189] de G , denotado $\text{Ta}_p(G)$, que é um $\mathbb{Z}_p$ -módulo topológico com uma topologia similar à topologia p -ádica de $\mathbb{Z}_p$. Observe que

$$\text{Ta}_p(G)/p\text{Ta}_p(G) \cong G[p].$$

Definição 4.3.32. Seja M um $\mathbb{Z}_p$ -módulo localmente compacto. O $\mathbb{Z}_p$ -**coposto** de M é o $\mathbb{Z}_p$ -posto de $\widehat{M}$. Dizemos que M é **cofinitamente gerado** se seu $\mathbb{Z}_p$ -coposto é finito.

A princípio, não é fácil dizer se um $\mathbb{Z}_p$ -módulo é cofinitamente gerado. Em casos específicos (e, não coincidentemente, no nosso, como veremos a seguir!), temos um resultado que facilita esta tarefa:

Lema 4.3.33 (Nakayama). Seja X um $\mathbb{Z}_p$ -módulo compacto. Um conjunto finito $S = \{x_1, \dots, x_d\}$ gera X se, e somente se, $\bar{S} = \{\bar{x}_1, \dots, \bar{x}_d\}$ é uma base para o $\mathbb{F}_p$ -espaço vetorial X/pX . Em particular, X é finitamente gerado se, e somente se, X/pX é finito (GREENBERG, 2010, p. 77, Proposição 2.2.1).

Assumiremos, por fim, o seguinte resultado de Álgebra Comutativa:

^[188]O isomorfismo é dado por $f \mapsto (f|_{G[p]}, f|_{G[p^2]}, f|_{G[p^3]}, \dots)$, e os mapas do limite inverso são as multiplicações por potências de p adequadas.

^[189]Recorde o módulo de Tate p -ádico de uma curva elíptica sobre $\mathbb{Q}$ definido na seção 3.4.

Teorema 4.3.34 (da Estrutura de Módulos Finitamente Gerados sobre um Domínio de Ideais Principais). Seja R um domínio de ideais principais e M um módulo finitamente gerado sobre R . Então, existem ideais próprios $(d_1) \supseteq (d_2) \supseteq \dots \supseteq (d_n)$ de R tais que

$$M = R^m \oplus \bigoplus_{i=1}^n R/(d_i)$$

(DUMMIT; FOOTE, 2004, p. 462, Teorema 5).

Proposição 4.3.35. Um $\mathbb{Z}_p$ -módulo localmente compacto cofinitamente gerado M tem a seguinte estrutura como $\mathbb{Z}_p$ -módulo:

$$M \cong (\mathbb{Q}_p/\mathbb{Z}_p)^s \oplus T,$$

com $s \in \mathbb{Z}_{\geq 0}$ e T é um p -grupo abeliano finito.

Prova. Como M é cofinitamente gerado, $\widehat{M}$ é um $\mathbb{Z}_p$ -módulo finitamente gerado. Como $\mathbb{Z}_p$ é um domínio de ideais principais (Teorema 1.4.12), pelo Teorema 4.3.34,

$$\widehat{M} \cong \mathbb{Z}_p^s \oplus T,$$

onde T é um p -grupo abeliano. Assim, pela Proposição 4.3.29,

$$M \cong \widehat{\widehat{M}} \cong \widehat{\mathbb{Z}_p^s} \oplus \widehat{T} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^s \oplus T. \quad \blacksquare$$

Finalmente, estamos prontos para começar a estudar a estrutura do p^∞ -grupo de Selmer.

Proposição 4.3.36. A sequência exata de p^∞ -descida cinde, isto é,

$$\text{Sel}_{p^\infty}(E) = (E(\mathbb{Q}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)) \oplus \text{III}(E)[p^\infty].$$

Prova. Segue da Proposição 1.3.3, pois $E(\mathbb{Q}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{r_{\text{alg}}(E)}$ é divisível. ■

Proposição 4.3.37. O $\mathbb{Z}_p$ -coposto de $\text{Sel}_{p^\infty}(E)$, denotado $r_p(E)$, é limitado pelo p -posto de Selmer $s_p(E)$, que é finito.

Prova. Como

$$(\text{Sel}_{p^\infty}(E))[p^e] \cong \text{III}(E)[p^e] \oplus (E(\mathbb{Q}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p))[p^e] \cong \text{III}(E)[p^e] \oplus (\mathbb{Z}/p^e\mathbb{Z})^{r_{\text{alg}}(E)},$$

temos que $\dim_{\mathbb{F}_p}((\text{Sel}_{p^\infty}(E))[p^e]) = \dim_{\mathbb{F}_p}(\text{III}(E)[p^e]) + e \cdot r_{\text{alg}}(E) \leq \dim_{\mathbb{F}_p}(\text{Sel}_{p^e}(E))$. Em particular, $(\text{Sel}_{p^\infty}(E))[p^e]$ é um grupo finito para todo $e \in \mathbb{N}$.

Pelo Exemplo 4.3.31, $X \doteq \widehat{\text{Sel}_{p^\infty}(E)} \cong \text{Ta}_p(\text{Sel}_{p^\infty}(E))$, o módulo de Tate p -ádico deste grupo. Assim,

$$X/pX \cong \text{Ta}_p(\text{Sel}_{p^\infty}(E))/p\text{Ta}_p(\text{Sel}_{p^\infty}(E)) \cong (\text{Sel}_{p^\infty}(E))[p]$$

é finito. Pelo Lema 4.3.33, X é um $\mathbb{Z}_p$ -módulo finitamente gerado. ■

Corolário 4.3.38. A parte p -primária do grupo de Tate–Shafarevich de E tem a seguinte estrutura como $\mathbb{Z}_p$ -módulo:

$$\text{III}(E)[p^\infty] = (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus T \oplus T$$

onde $r \in \mathbb{Z}_{\geq 0}$ e T é um p -grupo abeliano finito.

Prova. Considere o subgrupo $\text{III}(E)[p^\infty]_{\text{div}}$ dos elementos divisíveis. Pelo Corolário 1.3.6, temos que^[190]

$$\text{III}(E)[p^\infty]_{\text{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{(I_p)}.$$

Por ser um subgrupo de $\text{Sel}_{p^\infty}(E)$, $\text{III}(E)[p^\infty]_{\text{div}}$ tem $\mathbb{Z}_p$ -coposto finito, isto é, $\#I_p = r < \infty$.

Quanto à parte não-divisível, $\text{III}(E)[p^\infty]_{\text{nd}}$ é finito, pela Proposição 4.3.35. Logo, o pareamento de Cassels (Teorema 4.3.18) se restringe a um pareamento não-degenerado neste subgrupo, donde $\text{III}(E)[p^\infty]_{\text{nd}} \cong T \oplus T$, onde T é um p -grupo abeliano finito. ■

Corolário 4.3.39. O p^∞ -grupo de Selmer de E tem a seguinte estrutura como $\mathbb{Z}_p$ -módulo:

$$\text{Sel}_{p^\infty}(E) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{r_p(E)} \oplus T \oplus T,$$

onde T é um p -grupo abeliano finito.^[191]

Observação 4.3.40. Segue dos resultados anteriores que $s_p(E) \geq r_p(E) \geq r_{\text{alg}}(E)$. Como a parte p -primária do grupo de Tate–Shafarevich é conjecturalmente finita, é esperado que $r_p(E) = r_{\text{alg}}(E)$ e $\text{III}(E)[p^\infty] = \text{III}(E)[p^\infty]_{\text{nd}} = T \oplus T$. Como vimos na subseção 4.3.3, também esperamos que $s_p(E) = r_{\text{alg}}(E)$ quase sempre (a trivialidade do grupo de Tate–Shafarevich não é suficiente, pois $s_p(E)$ pode receber contribuições de $E(\mathbb{Q})[p]$).

Se a estrutura de $E(\mathbb{Q})$ for simples o suficiente, a relação entre os p^∞ e p -grupos de Selmer fica bem mais clara:

Proposição 4.3.41. Se $E(\mathbb{Q})[p] = 0$, então $\text{Sel}_{p^\infty}(E)[p] \cong \text{Sel}_p(E)$.

Prova. Seja $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A sequência exata

$$0 \longrightarrow E[p] \longrightarrow E[p^n] \xrightarrow{p} E[p^{n-1}] \longrightarrow 0$$

induz a sequência exata (Proposição 1.2.9)

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(\mathbb{Q})[p] & \xrightarrow{0} & E(\mathbb{Q})[p^n] & \xrightarrow{0} & E(\mathbb{Q})[p^{n-1}] & \xrightarrow{0} & 0 \\ & & \searrow & & \searrow & & \searrow & & \\ & & & & \delta & & & & \\ & & \hookrightarrow & H^1(G, E[p]) & \longrightarrow & H^1(G, E[p^n]) & \xrightarrow{\alpha} & H^1(G, E[p^{n-1}]) & \end{array}$$

^[190]Lembre que $(\mathbb{Q}/\mathbb{Z})[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$.

^[191]Este teorema é um outro bom motivo por que queremos que, na prática, $\text{III}(E)$ - ou, pelo menos, sua parte p -primária - seja trivial! Na verdade, basta que $\text{III}(E)$ seja finito: nesse caso, apenas para finitos primos $\text{III}(E)[p^\infty]$ é não-trivial. Escolha sua parte p -primária trivial favorita e seja feliz!

Componha α com a injeção $H^1(G, E[p^{n-1}]) \hookrightarrow H^1(G, E[p^n])$ induzida pela inclusão $E[p^{n-1}] \hookrightarrow E[p^n]$. O mapa $H^1(G, E[p^n]) \rightarrow H^1(G, E[p^n])$ induzido coincide com a multiplicação por p . Logo, $H^1(G, E[p]) \cong \ker(\alpha) = H^1(G, E[p^n])[p]$.

Por definição, um elemento de $H^1(G, E[p])$ pertence a $\text{Sel}_p(E)$ se, e somente se, se anula em $\text{WC}(E/\mathbb{Q}_p)$ para todo p . O mesmo acontece para $H^1(G, E[p^n])$. Logo, $\text{Sel}_p(E) \cong \text{Sel}_{p^n}(E)[p]$. Tomando o limite direto em n , concluímos que $\text{Sel}_{p^\infty}(E)[p] \cong \text{Sel}_p(E)$. ■

Encerramos a seção com um teorema muito importante a respeito de p^∞ -grupos de Selmer, que é uma consequência da chamada Conjectura Principal da Teoria de Iwasawa^[192].

Teorema 4.3.42 (Skinner–Urban). Seja $p \geq 3$ e E uma curva elíptica tal que

- E tem redução boa ordinária ou má multiplicativa em p ;
- $\bar{\rho}_{E,p}$ é irredutível (equivalentemente, $E(\mathbb{Q})[p] = 0$, pela Proposição 3.4.6);
- $\bar{\rho}_{E,p}$ ramifica em algum $\ell \neq p$ tal que $v_\ell(N_E) = 1$ (equivalentemente, E tem redução multiplicativa em algum $\ell \neq p$ tal que $p \nmid v_\ell(\Delta(E))$, pela Proposição 3.4.8).

Se $r_{\text{an}}(E) > 0$, então $r_p(E) \geq 1$. Em particular, se $r_{\text{an}}(E) > 0$, $\text{Sel}_{p^\infty}(E)$ é infinito.^[193]

^[192]A Conjectura Principal da Teoria de Iwasawa afirma essencialmente que os dois métodos comuns usados para se definir uma contraparte p -ádica das L -funções de curvas elípticas (a saber, por teoria de módulos e por interpolação) coincidem. Kato (2004), Skinner e Urban (2014) demonstraram esta conjectura para curvas elípticas com algumas restrições sobre suas representações de Galois. Para uma introdução a esta demonstração, veja Wan (2016).

^[193]Este enunciado combina dois resultados: Skinner e Urban (2014), p. 46, Teorema 3.6.11 (caso redução ordinária) e Skinner (2014b), p. 3, Teorema C (caso redução multiplicativa).

QUANTAS CURVAS ELÍPTICAS SATISFAZEM A CONJECTURA DE BIRCH E SWINNERTON-DYER?

Bom, esperamos que sejam todas. Mas enquanto não temos resposta para isto, mudemos a pergunta: para quantas curvas elípticas *sabemos* que a conjectura BSD é válida? Muitas ou poucas? Como medir esta quantidade?^[194]

Suponha que queiramos investigar determinada propriedade P sobre curvas elípticas (por exemplo, P pode ser “satisfazer a conjectura BSD”!). Uma maneira de atacar este problema é tentar calcular a probabilidade de uma curva elíptica E satisfazer P . Ou seja, tentamos calcular o quociente

$$\frac{\#\{\text{Curvas elípticas que satisfazem } P\}}{\#\{\text{Curvas elípticas}\}}.$$

Como existem infinitas curvas elípticas tanto no denominador quanto (provavelmente) no numerador, precisamos “quebrar” o quociente acima em pedaços finitos. A maneira mais comum de fazê-lo é associar a cada curva elíptica E um inteiro positivo $H(E)$, chamado **altura** de E , de modo que, para cada n positivo, apenas finitas E satisfaçam $H(E) \leq n$. Assim, o quociente anterior se torna

$$\lim_{n \rightarrow \infty} \frac{\#\{E; E \text{ satisfaz } P, H(E) \leq n\}}{\#\{E; H(E) \leq n\}},$$

e esta é a quantidade de curvas elípticas que satisfazem P quando ordenadas por altura H ^[195].

Porém, ainda é difícil calcular este quociente: mesmo que saibamos quantas curvas elípticas há no denominador da fração para cada n , saber quantas curvas elípticas há no numerador

^[194] Neste capítulo, toda curva elíptica, salvo menção em contrário, está definida sobre $\mathbb{Q}$.

^[195] Veja na próxima seção a definição precisa da altura que utilizaremos. Em alguns contextos, outras quantidades podem ser usadas, como o determinante ou o condutor de um modelo minimal global. A vantagem da altura (em detrimento do condutor, por exemplo, que é o preferido ao ordenar curvas elípticas em bancos de dados), é que temos controle sobre seu crescimento, como veremos a seguir.

deve ser quase tão complicado quanto atacar o problema diretamente. Por isso, em vez de calcular exatamente o quociente, *estimamo-lo* com cotas inferiores ou superiores.

Baseados nessa abordagem, [Bhargava, Skinner e Zhang \(2014\)](#) obtiveram uma notável cota inferior para a quantidade de curvas elípticas que satisfazem a Conjectura BSD:

Teorema BSZ (Bhargava–Skinner–Zhang). Temos que

$$\liminf_{n \rightarrow \infty} \frac{\#\{E; r_{\text{an}}(E) = r_{\text{alg}}(E) \leq 1, \#\text{III}(E) < \infty, H(E) \leq n\}}{\#\{E; H(E) \leq n\}} > 66,48\%.$$

Ou seja, quando ordenadas por altura, *a maioria das curvas elípticas satisfaz BSD!*^[196]

A prova deste resultado é sustentada por três teoremas centrais: dois deles (Teoremas [Zero](#) e [Um](#)) impõem condições p -ádicas (algumas muito restritivas, outras nem tanto – mas que podem ser medidas) para que uma curva elíptica E satisfaça $r_{\text{an}}(E) = r_{\text{alg}}(E) \in \{0, 1\}$, e o terceiro (Teorema [Dois](#)) ajuda a medir o quão restritivas são as condições impostas por aqueles dois teoremas sobre os p -grupos de Selmer de E . Para obter a cota inferior de 66,48%, impomos uma condição de cada vez e medimos a proporção correspondente ao subconjunto de curvas elípticas resultante.

Este capítulo está organizado da seguinte forma:

- Na seção [5.1](#), formalizamos o procedimento de contagem de curvas elípticas ordenadas por altura, além de apresentar todas as outras ferramentas que utilizaremos para discutir o artigo *A majority of elliptic curves satisfies the Birch and Swinnerton-Dyer conjecture*, de [Bhargava, Skinner e Zhang \(2014\)](#);
- Na seção [5.2](#), já com todo o vocabulário necessário, discutimos com mais detalhes a estratégia da prova do Teorema [BSZ](#);
- Na seção [5.3](#), enunciamos os três teoremas ([Zero](#), [Um](#) e [Dois](#)) que, como comentamos acima, serão fundamentais para a demonstração;
- Finalmente, na seção [5.4](#), concluímos a prova do Teorema [BSZ](#).

A referência básica deste capítulo será, evidentemente, o artigo de [Bhargava, Skinner e Zhang \(2014\)](#).

^[196]Mais do que isso, elas também satisfazem $r_{\text{an}}(E), r_{\text{alg}}(E) \leq 1$ e a Conjectura de Tate–Shafarevich ([4.3.16](#))!

5.1 Contando curvas elípticas sobre $\mathbb{Q}$

Toda curva elíptica E sobre $\mathbb{Q}$ é isomorfa a um modelo da forma $y^2 = x^3 + Ax + B$. Com alguns ajustes, podemos transformar esta equação na de um modelo “quase minimal global”^[197]:

Proposição 5.1.1. Uma curva elíptica E sobre $\mathbb{Q}$ é isomorfa a um único modelo da forma $E_{A,B}: y^2 = x^3 + Ax + B$, com A e B inteiros tais que $p^4 \mid A \implies p^6 \nmid B$ para todo p primo. Este modelo é p -minimal para todo $p \geq 5$.

Demonstração. Recorde que um isomorfismo entre duas curvas elípticas $E: y^2 = x^3 + Ax + B$ e $E': (y')^2 = (x')^3 + A'x' + B'$ é dado por

$$\begin{cases} x = u^2 x' \\ y = u^3 y' \end{cases},$$

com $u \in \mathbb{Q}^\times$. Com isto, é fácil eliminar os denominadores dos coeficientes da equação que define E , obtendo $A, B \in \mathbb{Z}$. Um isomorfismo desta forma influencia as constantes c_4 e c_6 de cada curva elíptica da seguinte maneira:

$$c_4 = c'_4 u^4 \quad \text{e} \quad c_6 = c'_6 u^6.$$

Como $A = -27c_4$ e $B = -54c_6$, temos que

$$A = A' u^4 \quad \text{e} \quad B = B' u^6.$$

Seja p primo tal que $p^4 \mid A$ e $p^6 \mid B$. Aplicando o isomorfismo com $u = p$, podemos eliminar estas potências excedentes. Repetindo este processo finitas vezes (pois A e B têm finitos divisores), obtemos para E um modelo $E_{A,B}$ nas condições do enunciado.

Para a unicidade, note que, se $E_{A,B} \cong E_{A',B'}$, então existe $u \in \mathbb{Q}^\times$ tal que

$$A = A' u^4 \quad \text{e} \quad B = B' u^6.$$

Se p é um primo no numerador de u , como $A, B, A', B' \in \mathbb{Z}$, $p^4 \mid A$ e $p^6 \mid B$, contradizendo a definição de $E_{A,B}$. Similarmente, se p é um primo no denominador de u , $p^4 \mid A'$ e $p^6 \mid B'$, contradizendo a definição de $E_{A',B'}$. Logo, $u = \pm 1 \implies A = A'$ e $B = B'$.

Finalmente, a minimalidade segue do critério 2.4 da seção 2.2, pois, para todo $p \geq 5$, $v_p(c_4) = v_p(A)$ e $v_p(c_6) = v_p(B)$. ■

De agora em diante, a menos de menção em contrário, vamos supor que toda curva elíptica sobre $\mathbb{Q}$ está no modelo “quase minimal global” $E_{A,B}$ descrito acima.

^[197]Um modelo dessa forma dificilmente será minimal global: por exemplo, como o discriminante dessa equação já vem penalizado com um fator -16 , esse modelo não será 2-minimal para nenhuma curva elíptica com redução boa em 2.

Definição 5.1.2. Definimos a **altura (naïve)** de $E_{A,B}$ por

$$H(E_{A,B}) \doteq \max\{4|A|^3, 27B^2\}.$$

Assim como as funções de altura do Capítulo 3, o conjunto $\{E; H(E) \leq n\}$ é finito para todo n :

Proposição 5.1.3. $\#\{E; H(E) \leq n\} \sim n^{5/6}$ à medida que $n \rightarrow \infty$ (BRUMER, 1992, Lema 4.3).

(Essencialmente, a condição $4|A|^3 \leq n$ contribui, na limitação assintótica acima, com $n^{1/3}$ e $27B^2 \leq n$ contribui com $n^{1/2}$.)

Seja P uma propriedade referente a curvas elípticas sobre $\mathbb{Q}$. Dizemos que $X\%$ das curvas elípticas satisfazem P **quando ordenadas por altura** se

$$\lim_{n \rightarrow \infty} \frac{\#\{E; E \text{ satisfaz } P, H(E) \leq n\}}{\#\{E; H(E) \leq n\}} = X\%$$

Às vezes, não se sabe se o limite existe. Neste caso, pode-se falar em cotas superiores e inferiores para a proporção de curvas elípticas que satisfazem P , trocando-se $\lim$ por $\limsup$ e $\liminf$, respectivamente.

5.1.1 Famílias de curvas elípticas

Definição 5.1.4. Seja ℓ primo. A **medida de Haar (normalizada)** em $\mathbb{Z}_\ell$ é a medida de Borel μ_ℓ dada pelas seguintes propriedades:

- $\mu_\ell(U) > 0$ para todo aberto U não-nulo;
- (Invariância por translação) $\mu_\ell(z + B) = \mu_\ell(B)$, para todo $z \in \mathbb{Z}_\ell$ e B conjunto de Borel;
- (Normalização) $\mu_\ell(\mathbb{Z}_\ell) = 1$.

Segue da Teoria da Medida em grupos localmente compactos que a medida acima existe (HALMOS, 1950, p. 254, Teorema B) e é única (*ibid.*, p. 263, Teorema C).

Suponha que queiramos calcular a medida do conjunto $S = \bigcup_{i=1}^N (\alpha_i + \ell^k \mathbb{Z}_\ell)$ obtido escolhendo-se N classes módulo ℓ^k . A medida μ_ℓ funciona exatamente como esperamos, como uma “probabilidade”:

$$\mu_\ell(S) = \sum_{i=1}^N \mu_\ell(\alpha_i + \ell^k \mathbb{Z}_\ell) = N \cdot \underbrace{\mu_\ell(\ell^k \mathbb{Z}_\ell)}_{=\mu_\ell(i + \ell^k \mathbb{Z}_\ell), \forall i} = N \cdot \frac{\sum_{i=1}^{\ell^k} \mu_\ell(i + \ell^k \mathbb{Z}_\ell)}{\ell^k} = N \cdot \frac{\mu_\ell(\mathbb{Z}_\ell)}{\ell^k} = \frac{N}{\ell^k}.$$

Assim, equipamos $\mathbb{Z}_\ell^2$ com a topologia produto induzida pela topologia ℓ -ádica e a medida produto induzida pela medida de Haar.

Uma **família** é qualquer conjunto de curvas elípticas. O seguinte tipo de família nos será de particular interesse:

Definição 5.1.5. Para cada ℓ , seja $\Sigma_\ell \subseteq S_\ell \doteq \{(A, B) \in \mathbb{Z}_\ell^2; \Delta(A, B) \neq 0\}$ um fechado com fronteira de medida nula e $\Sigma = (\Sigma_\ell)_\ell$, onde $\Delta(A, B) \doteq 4A^3 + 27B^2$. A **família** de curvas elípticas **associada a Σ** é o conjunto

$$F_\Sigma \doteq \{E_{A,B}; (A, B) \in \mathbb{Z} \text{ e } (A, B) \in \Sigma_\ell \forall \ell\}.$$

As condições impostas na definição da família são chamadas **condições de congruência**. Assim, dizemos que F_Σ é uma **família definida por condições de congruência**. Alguns exemplos comuns de condições de congruência são $v_\ell(\Delta(A, B)) = k$ (resp. $\leq$ ou $\geq$), $\ell \nmid A$, $A \equiv N \pmod{\ell^k}$ (resp. B), e assim por diante.

Definição 5.1.6. Uma família definida por condições de congruência F_Σ é **grande** se, para todo ℓ primo suficientemente grande, Σ_ℓ contém todas as curvas elípticas $E_{A,B}$ tais que $\ell^2 \nmid \Delta(A, B)$.

Em particular, intersecções finitas de famílias grandes são famílias grandes. Os principais exemplos de famílias grandes são as famílias definidas por finitas condições de congruência e, entre elas, o conjunto de todas as classes de isomorfismo de curvas elípticas.

Definimos a **densidade** de uma família F qualquer por

$$\mu(F) \doteq \lim_{n \rightarrow \infty} \frac{\#\{E \in F; H(E) \leq n\}}{\#\{E; H(E) \leq n\}}.$$

Se $F = F_\Sigma$ está definida por condições de congruência, também definimos sua **densidade local** em ℓ por

$$\mu_\ell(F_\Sigma) = \frac{\mu_\ell(\Sigma_\ell)}{\mu_\ell(\{(A, B) \in \mathbb{Z}_\ell^2; \ell^4 | A \implies \ell^6 \nmid B\})} = \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \mu_\ell(\Sigma_\ell),$$

ou seja, das curvas elípticas ℓ -integrals (as que satisfazem $\ell^4 | A \implies \ell^6 \nmid B$), consideramos a probabilidade destas serem dadas por um par $(A, B) \in \Sigma_\ell$.

Em princípio, não é possível calcular a densidade de uma família diretamente pela definição. Porém, se a família em questão é *grande*, esta densidade “global” pode ser obtida a partir das densidades locais, que são mais fáceis de se calcular na prática:

Proposição 5.1.7. Seja F uma família grande^[198]. Então,

$$\mu(F) = \prod_{\ell \text{ primo}} \mu_\ell(F)$$

(BHARGAVA; SHANKAR, 2013c, p. 31, seção 3.5).

^[198]Só ser definida por condições de congruência não basta: a prova deste resultado menciona explicitamente a condição que define família grande.

Em outras palavras, podemos considerar as condições de congruência impostas por cada primo separadamente e, se F está definida por condições de congruência módulo apenas um primo ℓ , $\mu(F) = \mu_\ell(F)$.

5.1.2 Root numbers

“Reduzindo a Conjectura BSD módulo 2”, obtemos a Conjectura da Paridade:

Conjectura 5.1.8 (Paridade). Seja E uma curva elíptica. Então, $r_{\text{alg}}(E) \equiv r_{\text{an}}(E) \pmod{2}$.

Esta conjectura foi verificada em alguns casos que assumiam certas hipóteses sobre o grupo de Tate–Shafarevich de E (DOKCHITSER, 2012). Por exemplo, a finitude de $\text{III}(E)$ é uma condição suficiente para que E satisfaça a Conjectura da Paridade:

Teorema 5.1.9 (Monsky). Se $\#\text{III}(E) < \infty$, $r_{\text{alg}}(E) \equiv r_{\text{an}}(E) \pmod{2}$ (MONSKY, 1996).

Seja E uma curva elíptica. Pelo Teorema da Modularidade (Teorema 3.2.3), existe uma forma modular f_E cuja L -função coincide com a de E . Tal L -função satisfaz uma equação funcional (Proposição 1.8.4)

$$\Lambda(s, f_E) = w_E \Lambda(2 - s, f_E), \quad \text{onde } \Lambda(s, f_E) = \frac{N_E^{s/2}}{(2\pi)^s} \Gamma(s) L(s, f_E),$$

com $w_E \in \{\pm 1\}$

Definição 5.1.10. O número $w_E \in \{\pm 1\}$ acima é chamado *root number* de E .^[199]

Observe que a ordem de $L(s, f_E)$ em $s = 1$ é a mesma de $\Lambda(s, f_E)$. Assim,

$$L^{(r_{\text{an}}(E))}(1, f_E) = w_E (-1)^{r_{\text{an}}(E)} L^{(r_{\text{an}}(E))}(1, f_E) \implies w_E = (-1)^{r_{\text{an}}(E)}.$$

Isto mostra a seguinte proposição:

Proposição 5.1.11 (Paridade do posto analítico). Seja E uma curva elíptica. Então, $r_{\text{an}}(E)$ é par se, e somente se, $w_E = 1$.

Em particular, obtemos uma reformulação para a Conjectura da Paridade:

Conjectura 5.1.12 (Paridade). Seja E uma curva elíptica. Então, $r_{\text{alg}}(E)$ é par se, e somente se, $w_E = 1$.

Outras quantidades associadas a curvas elípticas, como seu p -posto de Selmer e o $\mathbb{Z}_p$ -coposto de $\text{Sel}_{p^\infty}(E)$ também estão associadas a seu *root number*^[200]:

^[199]Veja a seção A.2.1 para alguns exemplos.

^[200]Ambos números que também esperamos que sejam iguais a $r_{\text{alg}}(E)$!

Teorema 5.1.13 (p -Paridade). Seja E uma curva elíptica e $r_p(E)$ o $\mathbb{Z}_p$ -coposto do p^∞ -grupo de Selmer de E . Então, $r_p(E)$ é par, se e somente se, $w_E = 1$ (DOKCHITSER; DOKCHITSER, 2010, p. 593, Teorema 4.19).

Teorema 5.1.14. (Dokchitser–Dokchitser) Seja E uma curva elíptica, p primo e $s_p(E)$ o p -posto do p -grupo de Selmer de E . Então, $s_p(E) - \dim_{\mathbb{F}_p}(E(\mathbb{Q})[p])$ é par se, e somente se, $w_E = 1$ (DOKCHITSER; DOKCHITSER, 2010).

Em outras palavras, a paridade de $s_p(E)$ é determinada pelo *root number* de E .

Conjectura-se, também, que o *root number*, e portanto, as paridades mencionadas acima (em particular, a do posto algébrico) estejam equidistribuídas:

Conjectura 5.1.15 (Equidistribuição). Quando ordenadas por altura, metade das curvas elípticas satisfazem $w_E = 1$, e a outra metade $w_E = -1$.

Pelo menos, é sabido que o *root number* é equidistribuído para a maioria das curvas elípticas, quando ordenadas por altura:

Teorema 5.1.16 (Bhargava–Shankar). Existe uma união finita $\mathcal{F}$ de famílias grandes^[201] definidas por condições de congruência módulo primos $\ell \equiv 1 \pmod{4}$, com densidade $\mu(\mathcal{F}) \doteq \kappa > 55,01\%$, onde o *root number* é equidistribuído (BHARGAVA; SHANKAR, 2013b, p. 4, Teorema 6).

A família $\mathcal{F}$ é construída de modo que, para cada $E \in \mathcal{F}$, $E_{-1} \in \mathcal{F}$, onde

$$E_{-1}: y^2 = x^3 + Ax - B$$

é o (-1) -*twist* de E . Como $w_E w_{E_{-1}} = -1$ e $H(E) = H(E_{-1})$, para cada curva elíptica com *root number* 1, existe uma com *root number* -1 na mesma altura e vice-versa, o que garante a equidistribuição do *root number* em $\mathcal{F}$.

Corolário 5.1.17. Se F é um família grande definida por condições de congruência módulo primos $\ell \equiv 1 \pmod{4}$, $F' = F \cap \mathcal{F}$ é uma união finita de subfamílias grandes de F onde o *root number* é equidistribuído e $\mu(F') = \kappa \mu(F)$.

Na prática, esta é a maior subfamília conhecida de uma família grande “genérica” onde podemos garantir equidistribuição do *root number*.

^[201]Uma união (mesmo finita) de famílias grandes pode não ser uma família grande.

5.1.3 O posto algébrico médio

Por posto algébrico médio, com as curvas elípticas ordenadas por altura, entendemos^[202]

$$\lim_{n \rightarrow \infty} \frac{\sum_{H(E) \leq n} r_{\text{alg}}(E)}{\sum_{H(E) \leq n} 1}.$$

Historicamente, a abordagem por estimativas e proporções que apresentamos parece ter se originado das tentativas de se estimar o posto algébrico médio: assumindo a Hipótese de Riemann Generalizada (Conjectura 1.8.2), foram obtidas algumas cotas superiores para o posto *analítico* médio que, assumida a conjectura BSD, se traduzem em cotas superiores para o posto *algébrico* médio. As cotas obtidas foram:

- Brumer (1992): 2,3;
- Heath-Brown (2003): 2;
- Young (2004): $\frac{25}{14} \approx 1,79$.

Em 2013, Bhargava e Shankar publicaram uma nova abordagem ao problema que não assumia nem a Hipótese de Riemann Generalizada nem a Conjectura BSD^[203]. Empregando apenas técnicas algébricas, as cotas superiores que eles obtiveram foram:

- Bhargava e Shankar (2013c): 1,5 (caso $p = 2$);
- Bhargava e Shankar (2013d): $\frac{7}{6} \approx 1,17$ (caso $p = 3$);
- Bhargava e Shankar (2013b): $\approx 0,89$ (caso $p = 5$, primeira cota abaixo de 1!), menor cota até o momento.

As cotas se aproximam cada vez mais do seu valor esperado, que é 0,5:

Conjectura 5.1.18. O posto algébrico médio das curvas elípticas sobre $\mathbb{Q}$ é $\frac{1}{2}$.

Esta conjectura é consequência de uma outra conjectura “folclórica”:

Conjectura 5.1.19 (Goldfeld–Katz–Sarnak). Em algum sentido, 50% das curvas elípticas possuem posto 0, 50% possuem posto 1 e 0% possuem posto ≥ 2 .

^[202]Não se sabe se o limite abaixo sempre existe. Portanto, para estimar o posto algébrico médio por cima, substitui-se $\lim$ por $\limsup$, para se obter uma quantidade bem definida.

^[203]A abordagem foi tão revolucionária que Bhargava ganhou a medalha Fields em 2014!

Portanto, espera-se que as curvas elípticas tenham posto baixo, em geral, que são justamente os casos sobre os quais temos mais informações!^[204]

Observação 5.1.20. Recorde a pergunta posta no início do Capítulo 3. Se a Conjectura 5.1.19 for verdadeira, o caso $g = 1$ é o perfeito meio-termo entre os casos $g = 0$ (todas as curvas possuindo infinitos pontos $\mathbb{Q}$ -racionais) e $g \geq 2$ (todas as curvas possuindo finitos pontos $\mathbb{Q}$ -racionais)!

5.2 A estratégia da prova

O roteiro da prova do Teorema BSZ é o seguinte:

- Existem dois Teoremas (Zero e Um, ver seção 5.3) que impõem diversas condições p -ádicas para que uma curva elíptica satisfaça $r_{\text{an}}(E) = r_{\text{alg}}(E) = 0$ ou 1. Partindo do conjunto de todas as curvas elípticas, impomos uma condição de cada vez, e calculamos a densidade do subconjunto resultante, com as curvas elípticas ordenadas por altura;
- Algumas condições (a saber, (ii) e (iii) do Teorema Zero e (ii) e (iv) do Teorema Um) valem para 100% das curvas elípticas (Proposição 5.3.2). Como estamos interessados apenas em porcentagens de curvas elípticas, podemos ignorar estas duas condições, que serão automaticamente satisfeitas;
- Cada teorema também impõe uma condição sobre o tamanho do p -grupo de Selmer (a saber, (iv) do Teorema Zero e (vi) do Teorema Um). Aqui entra o terceiro teorema central da prova, o Teorema Dois, que determina a ordem média dos p -grupos de Selmer, a partir da qual obtemos as proporções de curvas elípticas numa família (qualquer!) que satisfazem aquelas condições. Além disso, se soubermos que tal família possui *root number* equidistribuído, as proporções melhoram (Proposições 5.3.9 e 5.3.10, Teorema 5.3.11). A partir daqui, somos obrigados a tomar $p = 5$, pois este é o único caso onde valem simultaneamente os Teoremas Zero, Um e Dois;
- Restam três condições, que dão origem a três famílias grandes encaixantes cujas densidades conseguimos ser calculadas (Proposições 5.4.2, 5.4.3 e 5.4.7);
- Finalmente, impomos sobre estas famílias as condições sobre o p -grupo de Selmer dadas pelas proporções obtidas a partir do Teorema Dois. No fim, concluímos que 66,48% das curvas elípticas satisfazem $r_{\text{an}}(E) = r_{\text{alg}}(E) \leq 1$, donde também satisfazem as Conjecturas BSD (diretamente) e de Tate–Shafarevich (pelo Teorema de Kolyvagin–Rubin, 4.3.17).

^[204]Curiosamente, apesar de se esperar, com fundamentação teórica, que o posto algébrico médio seja $1/2$, os dados computacionais acumulados pelo estudo de diversas famílias de curvas elípticas parecem indicar que o posto algébrico médio se aproxima de $2/3$. Esse interessante conflito é discutido detidamente no artigo de [Bektemirov et al. \(2007\)](#).

5.3 Três teoremas importantes

Nesta seção, apresentamos os três teoremas que, como viemos enfatizando (bastante) até aqui, são a alma da prova do Teorema BSZ. O primeiro deles determina condições p -ádicas suficientes para que uma curva elíptica tenha postos algébrico e analítico iguais a 0 e é uma consequência direta do Teorema de Skinner–Urban (4.3.42):

Teorema Zero (Skinner–Urban). Seja $p \geq 5$ primo e E uma curva elíptica tal que

- (i) E tem redução boa ordinária ou má multiplicativa em p ;
- (ii) $\bar{\rho}_{E,p}$ é irredutível;
- (iii) $\bar{\rho}_{E,p}$ ramifica em algum $\ell \neq p$ tal que $v_\ell(N_E) = 1$;
- (iv) $\text{Sel}_p(E)$ é trivial.

Então, $r_{\text{alg}}(E) = r_{\text{an}}(E) = 0$.

Prova. Por (ii), $E(\mathbb{Q})[p] = 0$ (Proposição 3.4.6), donde $\text{Sel}_{p^\infty}(E)[p] = \text{Sel}_p(E) = 0$ (Proposição 4.3.41). Pela Observação 4.3.40, $0 = s_p(E) \geq r_p(E) \geq r_{\text{alg}}(E) \implies r_{\text{alg}}(E) = r_p(E) = 0$. Logo, $\text{Sel}_{p^\infty}(E) = T \oplus T$, onde T é um p -grupo finito. Como a p -torção de $\text{Sel}_{p^\infty}(E)$ é trivial, $T = 0$, donde $\text{Sel}_{p^\infty}(E) = 0$. Pelo (outro) Teorema de Skinner–Urban (4.3.42), $r_{\text{an}}(E) = 0$. ■

O segundo deles, similarmente, nos dá condições p -ádicas suficientes para que uma curva elíptica tenha postos algébrico e analítico iguais a 1:

Teorema Um (Skinner–Zhang). Seja $p \geq 5$ primo e E uma curva elíptica tal que

- (i) E tem redução boa ordinária ou má multiplicativa em p ;
- (ii) $\bar{\rho}_{E,p}$ é irredutível;
- (iii) $\bar{\rho}_{E,p}$ ramifica em todo $\ell \equiv \pm 1 \pmod{p}$ tal que $v_\ell(N_E) = 1$;
- (iv) Se N_E não é livre de quadrados^[205], então existem pelo menos dois primos $\ell \neq p$ distintos tais que $v_\ell(N_E) = 1$ em que $\bar{\rho}_{E,p}$ ramifica;
- (v) Se E tem redução multiplicativa em p , então $p \nmid v_p(\Delta(E))$. Se, além disso, a redução for *split*, então $v_p(\mathcal{L}_p(E)) = 1$;
- (vi) $\text{Sel}_{p^\infty}(E) = \mathbb{Q}_p/\mathbb{Z}_p$. Em particular, $r_p(E) = 1$.

^[205]Isto é, E tem redução aditiva em algum lugar.

Então, $r_{\text{alg}}(E) = r_{\text{an}}(E) = 1$ (ZHANG, 2014, p. 6, Teorema 1.4 (i)), (SKINNER; ZHANG, 2014, p. 3, Teorema 1.1).

A hipótese (vi) pode ser difícil de se verificar. Portanto, trocamos-la por uma mais simples:

Teorema 5.3.1. No teorema acima, podemos trocar (vi) por

(vi') $\text{Sel}_p(E)$ tem ordem p .

Prova. Como $s_p(E) = 1$ por (vi'), temos que $r_p(E) \leq 1$. Pelo Corolário 4.3.39,

$$\text{Sel}_{p^\infty}(E) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{r_p(E)} \oplus T \oplus T,$$

onde T é um p -grupo abeliano finito. Por (ii), $E(\mathbb{Q})[p] = 0$ (Proposição 3.4.6). Logo, $\text{Sel}_p(E)$ é o subgrupo de p -torção de $\text{Sel}_{p^\infty}(E)$ (Proposição 4.3.41). Como T é um p -grupo, se $T \neq 0$, existe um elemento a de ordem p , donde o subgrupo de ordem p^2 de $\text{Sel}_{p^\infty}(E)$ gerado por $(0, a, 0)$ e $(0, 0, a)$ estaria contido em $\text{Sel}_{p^\infty}(E)[p]$, mas isto não é possível, pois este grupo tem ordem p . Logo, $T = 0$. Como $\text{Sel}_{p^\infty}(E)$ é não trivial, $r_p(E) \neq 0 \implies r_p(E) = 1$, que é (vi). ■

Ambos os Teoremas 4.3.42 (do qual o Teorema Zero é consequência) e Um enunciados acima são resultados profundos e de difícil demonstração, e por isso, nos limitaremos a apenas remeter o leitor aos artigos onde foram provados.

Poderia-se perguntar se as condições pedidas nos teoremas acima não acabam sendo restritivas demais para serem satisfeitas por alguma proporção relevante de curvas elípticas. Na verdade, como veremos a seguir, não são: de fato, algumas delas valem quase sempre!

Proposição 5.3.2. Seja p primo. As seguintes propriedades são satisfeitas por 100% das curvas elípticas sobre $\mathbb{Q}$, quando ordenadas por altura:

- (i) $\bar{\rho}_{E,p}$ ramifica em pelo menos dois primos $\ell \neq p$ tais que $v_\ell(N_E) = 1$ [206];
- (ii) $\bar{\rho}_{E,p}$ é irredutível.

Na prova de (i), vamos usar uma consequência imediata da Fórmula de Ogg–Saito:

Lema 5.3.3 (Ogg–Saito). Seja p primo e E uma curva elíptica num modelo p -minimal. Se $v_p(\Delta(E)) = 1$, então $v_p(N_E) = 1$ (SILVERMAN, 2009, p. 450, Proposição C.16.2).

Esboço da prova de (i). Seja $L \geq 5$ um inteiro suficientemente grande. Para cada $\ell \neq p$ primo com $5 \leq \ell \leq L$, defina a família grande

$$S_\ell(L) = \{E_{A,B}; v_\ell(\Delta(E_{A,B})) \leq 1, 5 \leq q \leq L \text{ primo com } q \notin \{p, \ell\} \implies v_q(\Delta(E_{A,B})) \neq 1\}.$$

[206] Em particular, E tem redução multiplicativa em pelo menos dois primos diferentes de p .

Seja $S_\ell = \bigcap_{5 \leq L} S_\ell(L)$. Observe que $S = \bigcup_{5 \leq \ell, \ell \neq p} S_\ell$ é o conjunto de todas as curvas elípticas que não satisfazem (i): seja $E \notin S$ e $5 \leq \ell_0$ tal que $\ell_0 \nmid \Delta(E)$. Como $E \notin S_{\ell_0}$, existe $5 \leq \ell_1$ com $\ell_1 \notin \{p, \ell_0\}$ tal que $v_{\ell_1}(\Delta(E)) = 1$. Como $E \notin S_{\ell_1}$, repetimos o argumento obtendo $5 \leq \ell_2$ com $\ell_2 \notin \{p, \ell_1\}$ tal que $v_{\ell_2}(\Delta(E)) = 1$. Em particular, $v_{\ell_i}(N_E) = 1$, para $i = 1, 2$, pelo Lema 5.3.3. Assim, E tem redução multiplicativa em ℓ_1 e ℓ_2 . Pela Proposição 3.4.8, E satisfaz (i).

Afirmamos que S representa 0% das curvas elípticas sobre $\mathbb{Q}$. Como cada $S_\ell(L)$ está definido por finitas condições de congruência, é uma família grande. Pela Proposição 5.1.7,

$$\mu(S_\ell(L)) = \mu_\ell(S_\ell(L)) \cdot \prod_{5 \leq q \leq L, q \neq p, \ell} \mu_q(S_\ell(L)).$$

Vamos calcular os termos do produto.

Lema 5.3.4. Seja $\ell \geq 5$ primo. A medida do conjunto $(A, B) \in \mathbb{Z}_\ell^2$ tal que $v_\ell(\Delta(A, B)) = k$ para algum $k > 0$ e $\ell \nmid A$ é $\frac{(\ell-1)^2}{\ell^{k+2}}$.

Prova do Lema 5.3.4. Como a equação $(\frac{A}{3})^3 \equiv (\frac{B}{2})^2 \pmod{\ell^k}$ tem solução com $k > 0$, $A/3$ é um resíduo quadrático não-trivial módulo ℓ . Como $(\mathbb{Z}/\ell\mathbb{Z})^\times$ é cíclico, existem $\frac{\ell-1}{2}$ classes para A módulo ℓ nessas condições.

Para cada escolha de A , levante para uma classe módulo ℓ^{k+1} . Embutimos a condição restante na escolha de B : note que existem 2 classes módulo ℓ^k para B que satisfazem a equação acima. Estas se levantam para 2ℓ classes módulo ℓ^{k+1} , das quais 2 também resolvem a equação módulo ℓ^{k+1} . Removendo estas, obtemos $2\ell - 2$ opções para $B \pmod{\ell^{k+1}}$.

$$\text{Logo, a densidade deste conjunto é } \frac{\ell-1}{2\ell} \cdot \frac{2\ell-2}{\ell^{k+1}} = \frac{(\ell-1)^2}{\ell^{k+2}}. \quad \blacksquare$$

Continuação do esboço da prova de (i). Seja $q \notin \{\ell, p\}$. Se $v_q(\Delta(E)) = 1$, então $v_q(N_E) = 1$ (Lema 5.3.3), donde E tem redução multiplicativa em q e $q \nmid A$. Portanto, a densidade das curvas elípticas que satisfazem $v_q(\Delta(A, B)) \neq 1$ é dada pelo Lema 5.3.4:

$$\left(1 - \frac{1}{q^{10}}\right)^{-1} \left(1 - \frac{(q-1)^2}{q^3}\right).$$

Similarmente, para $\ell \neq p$, a densidade das curvas elípticas que satisfazem $v_\ell(\Delta(A, B)) \leq 1$ é

$$\left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(\frac{\ell-1}{\ell} + \frac{(\ell-1)^2}{\ell^3}\right) = \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \frac{1}{\ell^2} - \frac{\ell-1}{\ell^3}\right),$$

onde os termos somados são, respectivamente, os casos $k = 0$ e $k = 1$, que são disjuntos.

No artigo, conclui-se a prova deste lema (BHARGAVA; SKINNER; ZHANG, 2014, p. 11, Lema 20) considerando-se $S(L) = \bigcup_{5 \leq \ell \leq L, \ell \neq p} S_\ell(L)$ para todo L , donde $S = \bigcap_{5 \leq L} S(L)$. Assim,

$$\begin{aligned} \mu(S) &\stackrel{(*)}{=} \lim_{L \rightarrow \infty} \mu(S(L)) = \lim_{L \rightarrow \infty} \sum_{5 \leq \ell \leq L, \ell \neq p} \mu(S_\ell(L)) \\ &= \lim_{L \rightarrow \infty} \sum_{5 \leq \ell \leq L, \ell \neq p} \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \frac{1}{\ell^2} - \frac{\ell-1}{\ell^3}\right) \prod_{5 \leq q \leq L, q \notin \{\ell, p\}} \left(1 - \frac{1}{q^{10}}\right)^{-1} \left(1 - \frac{(q-1)^2}{q^3}\right) \\ &\stackrel{(**)}{=} 0. \end{aligned} \quad \blacksquare$$

Nota 5.3.5. As igualdades (*) e (**) não puderam ser verificadas. No primeiro caso, a desigualdade $\leq$ é sempre garantida, o que serviria para os propósitos desta demonstração caso (**) fosse verificada, mas a igualdade (*) teria que ser checada pela definição de μ , exigindo justificar uma troca de limites envolvendo uma sequência difícil (se não impossível) de descrever. Isto porque μ não é uma medida: o conjunto das classes de isomorfismos das curvas elípticas é enumerável e os conjuntos unitários têm densidade nula.

A igualdade (**) parece estar fundamentada na ideia de que o produto infinito diverge para zero. Porém, o produto diverge para zero muito lentamente (porque a possibilidade de E ter redução boa em $q \neq \ell, p$ impõe que os numeradores dos fatores sejam da ordem de crescimento $O(1)$) e, como os processos-limite da série do produto infinito ocorrem ao mesmo tempo, o limite tal como apresentado acima parece divergir, pois o limite do produto não consegue vencer o limite da soma, que, como o termo em ℓ também é $O(1)$, tem ordem de crescimento $O(L)$. Isto parece ser um problema na essência da abordagem pois, ainda que tomemos o conjunto exato das curvas elípticas que falham (i), continuamos com a mesma situação: produto de termos $O(1)$ divergindo pra zero, soma divergindo para ∞ com ordem $O(L)$.

Tentamos uma abordagem alternativa à dos autores do artigo, considerando os conjuntos S_ℓ definidos no começo da prova em vez dos $S(L)$ usados acima, de modo a “desconectar” estes processos-limite. Como

$$\begin{aligned} \mu(S_\ell) &= \lim_{L \rightarrow \infty} \mu(S_\ell(L)) \\ &= \lim_{L \rightarrow \infty} \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \frac{1}{\ell^2} - \frac{\ell-1}{\ell^3}\right) \prod_{5 \leq q \leq L, q \notin \{\ell, p\}} \left(1 - \frac{1}{q^{10}}\right)^{-1} \left(1 - \frac{(q-1)^2}{q^3}\right) \\ &= 0. \end{aligned}$$

esperava-se concluir que

$$\mu(S) = \mu\left(\bigcup_{5 \leq \ell, \ell \neq p} S_\ell\right) \stackrel{(?)}{\leq} \sum_{5 \leq \ell, \ell \neq p} \mu(S_\ell) = 0.$$

Porém, novamente pelo fato de μ não ser uma medida, a desigualdade (?) não pôde ser verificada.

Ideias da Prova de (ii). Pelo Teorema de Mazur (Teorema 3.1.2), $E(\mathbb{Q})_{\text{tor}}[p]$ é trivial para $p \geq 11$. Então, resta mostrar que 100% das curvas elípticas têm p -torção trivial para $p \in \{2, 3, 5, 7\}$. Para obter o 100%, usaremos o seguinte resultado:

Teorema 5.3.6 (da Irredutibilidade de Hilbert). Seja $f \in \mathbb{Q}[X_1, \dots, X_r, Y_1, \dots, Y_s]$ um polinômio irredutível. Então, existe $V \subseteq \mathbb{A}^r(\mathbb{Q})$ denso de Zariski tal que, para todo $(a_1, \dots, a_r) \in V$, $f(a_1, \dots, a_r, -) \in \mathbb{Q}[Y_1, \dots, Y_s]$ é irredutível (LANG, 1983, p. 225, Capítulo 9).

Seja $E: y^2 = x^3 + Ax + B$ uma curva elíptica “genérica” (isto é, definida sobre $\mathbb{Q}[A, B]$) e considere o n -ésimo polinômio de divisão $\psi_n \in \mathbb{Z}[A, B, x, y]$ de E , definido recursivamente por (WASHINGTON, 2008, p. 80, Seção 3.2)

$$\begin{aligned}\psi_0 &\doteq 0 \\ \psi_1 &\doteq 1 \\ \psi_2 &\doteq 2y \\ \psi_3 &\doteq 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \psi_4 &\doteq 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\ &\vdots \\ \psi_{2m+1} &\doteq \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2 \\ \psi_{2m} &\doteq \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3\end{aligned}$$

Se n é ímpar (em particular, 3, 5 ou 7), $\psi_n \in \mathbb{Z}[A, B, x]$ é irredutível. Se E é uma curva elíptica “concreta” (isto é, A e B são números racionais em vez de variáveis), as raízes de $\psi_n(A, B, x)$ são as abscissas dos pontos de n -torção de E . Se $n = 2$, as raízes de $f(A, B, x) = x^3 + Ax + B$ são as abscissas dos pontos de 2-torção de E .

Pelo Teorema da Irreducibilidade de Hilbert, o conjunto dos $(A, B) \in \mathbb{A}^2(\mathbb{Q})$ tais que $f(A, B, x)$ e $\psi_p(A, B, x)$ (para $p \in \{3, 5, 7\}$) são irredutíveis em $\mathbb{Q}[x]$ é denso de Zariski. Logo, 100% das curvas elípticas têm p -torção trivial, com $p \in \{2, 3, 5, 7\}$. Combinando estes (finitos) casos, concluímos que “quase todas” as curvas elípticas têm torção trivial. $\square$

Em particular, as hipóteses (ii) e (iii) do Teorema Zero e as hipóteses (ii) e (iv) do Teorema Um são satisfeitas por 100% das curvas elípticas sobre $\mathbb{Q}$.

5.3.1 As condições sobre os p -grupos de Selmer

As hipóteses (iv) do Teorema Zero e (vi') do Teorema Um tratam da ordem do p -grupo de Selmer. Se soubéssemos qual é a “ordem média dos p -grupos de Selmer” $\overline{S_p}$, definida em

algum sentido apropriado, teríamos que, sendo x_i a proporção das curvas elípticas sobre $\mathbb{Q}$ tais que $s_p(E) = i$ (ou seja, $\#\text{Sel}_p(E) = p^i$),

$$\sum_{i=0}^{\infty} p^i x_i = \overline{S}_p \quad \text{e} \quad \sum_{i=0}^{\infty} x_i = 1.$$

Em particular, estamos interessados em $i = 0, 1$. Em cada caso, aglutinando todos os outros termos da soma no termo de menor índice, perdemos informação, mas possivelmente, obtemos uma maneira de estimar a proporção de das curvas elípticas com p -posto de Selmer i :

$$p^0 x_0 + p(1 - x_0) \leq \overline{S}_p \iff x_0 \geq \frac{p - \overline{S}_p}{p - 1} \quad \text{e} \quad p^0(1 - x_1) + px_1 \leq \overline{S}_p \iff x_1 \leq \frac{\overline{S}_p - 1}{p - 1}.$$

Só há um problema: estas estimativas são fracas demais ou, até mesmo, triviais! Acabamos perdendo informação demais.

Mas nem tudo está perdido. O argumento acima pode ser feito em qualquer família F de curvas elípticas, não necessariamente grande, dado que conheçamos a “ordem média dos p -grupos de Selmer” $\overline{S}_p^F$ dentro de F . Na busca por restrições mas rígidas, pensamos na paridade. O Teorema de Dokchitser–Dokchitser (5.1.14) afirma que a paridade do p -posto de Selmer em qualquer família é controlada pelos *root numbers*. Em particular, se o *root number* for equidistribuído em F , $s_p(E)$ é par para 50% das $E \in F$ e ímpar para os outros 50%^[207]. Nesse caso, o cenário em F se torna

$$\sum_{i=0}^{\infty} p^i x_i^F = \overline{S}_p^F, \quad \sum_{\substack{i=0 \\ i \text{ par}}}^{\infty} x_i^F = \frac{1}{2} \quad \text{e} \quad \sum_{\substack{i=0 \\ i \text{ ímpar}}}^{\infty} x_i^F = \frac{1}{2}.$$

Pedir a equidistribuição do *root number*, que é apenas conjectural em geral, pode parecer um preço alto a se pagar, mas, as estimativas obtidas na prática adaptando o método anterior mostram que o sacrifício compensa.

$$p^0 x_0^F + p \frac{1}{2} + p^2 \left(\frac{1}{2} - x_0^F \right) \leq \overline{S}_p^F \iff x_0^F \geq \frac{p + p^2 - 2\overline{S}_p^F}{2(p^2 - p)}$$

$$p^0 \frac{1}{2} + px_1 + \left(\frac{1}{2} - x_1 \right) p^3 \leq \overline{S}_p^F \iff x_1^F \geq \frac{1 + p^3 - 2\overline{S}_p^F}{2(p^3 - p)}.$$

Como secretamente esperamos que $r_{\text{alg}}(E)$ esteja em torno de 1 e $s_p(E) = r_{\text{alg}}(E)$ quase sempre, esperamos também que $\overline{S}_p^F$ esteja em torno de p para qualquer F . Assim, as estimativas acima parecem, a princípio, serem não-triviais e, portanto, potencialmente úteis. Na verdade, como veremos a seguir, este parece ser um excelente chute para esse valor mas, antes, precisamos formalizar esse conceito de ordem média dos grupos de Selmer.

^[207]Lembrando que, pela Proposição 5.3.2, $\dim_{\mathbb{F}_p}(E(\mathbb{Q})[p]) = 0$ para 100% das curvas elípticas.

Definição 5.3.7. Seja F uma família grande de curvas elípticas. Por ordem média dos m -grupos de Selmer com as curvas elípticas ordenadas por altura, entendemos

$$\overline{S}_p^F \doteq \lim_{n \rightarrow \infty} \frac{\sum_{E \in F; H(E) < n} \# \text{Sel}_m(E)}{\sum_{E \in F; H(E) < n} 1}.$$

Como acabamos de comentar, secretamente esperamos que $\overline{S}_p^F$ esteja em torno de p . Porém, isto ainda é conjectura para a maioria dos casos:

Conjectura 5.3.8 (Bhargava). A ordem média dos m -grupos de Selmer $\text{Sel}_m(E)$ em qualquer família de curvas elípticas, com as curvas elípticas ordenadas por altura, é $\sum_{d|m} d$. Em particular, a ordem média dos p -grupos de Selmer $\text{Sel}_p(E)$ é $p + 1$.^[208]

Alguns casos dessa conjectura são conhecidos: ela foi verificada por Bhargava e Shankar nos casos $m \leq 5$ ^[209], revelando, em vista da técnica de estimativas que acabamos de descrever, o terceiro ingrediente principal da prova do Teorema **BSZ**:

Teorema Dois (Bhargava–Shankar). A conjectura de Bhargava vale para todo $m \leq 5$, isto é, a ordem média do m -grupo de Selmer em qualquer família grande de curvas elípticas, com as curvas elípticas ordenadas por altura, é

m	2	3	4	5
ordem média de $\text{Sel}_m(E)$	3	4	7	6

As provas destes teoremas se baseiam em identificar os elementos dos m -grupos de Selmer com espaços homogêneos C (sim, aqueles do Capítulo 4!) que possuem pontos racionais em todos os lugares (isto é, $C(\mathbb{Q}_p) \neq \emptyset$ para todo $p \leq \infty$), munidos de uma isogenia φ (Definição 2.1.9) de grau m^2 .^[210] Estes pares (C, φ) , por sua vez, são vistos como formas quárticas, que são contadas usando técnicas de Geometria dos Números, desenvolvidas pelos próprios autores dos artigos.

Voltemos às nossas estimativas. Como nosso interesse principal é estimar o quão restritivas são as condições sobre o p -grupo de Selmer impostas pelos Teoremas **Zero** e **Um**, somos obrigados a escolher $p = 5$ ^[211]. Vamos utilizar as técnicas que descrevemos anteriormente para

^[208]Veja Delaunay (2001) e Poonen e Rains (2011) para evidências heurísticas que apoiam a validade desta conjectura.

^[209]Veja Bhargava e Shankar (2013c) para o caso $p = 2$, Bhargava e Shankar (2013d) para o caso $p = 3$, Bhargava e Shankar (2013a) para o caso $m = 4$ e Bhargava e Shankar (2013b) para o caso $p = 5$.

^[210]Não comentamos neste trabalho, mas, para toda isogenia $\phi: E_1 \rightarrow E_2$, existe uma isogenia **dual** $\hat{\phi}: E_2 \rightarrow E_1$ tal que $\hat{\phi} \circ \phi = [m]$, para algum $m \in \mathbb{Z}_{>0}$. Nesse caso, dizemos que o **grau** de ϕ é m^2 .

^[211]Na verdade, pelas frações que aparecem nas estimativas, também parece que obtemos cotas inferiores mais “refinadas” quanto maior for p , então tomamos o maior dos casos conhecidos da Conjectura 5.3.8.

obter as estimativas para as proporções de curvas elípticas de p -posto de Selmer são 0 ou 1 dentro de uma família com *root number* equidistribuído F , começando pelo caso $s_p(E) = 0$:

Proposição 5.3.9. Seja F uma família de curvas elípticas com *root number* equidistribuído. Então, pelo menos $\frac{3}{8}$ das curvas elípticas em F , quando ordenadas por altura, têm 5-posto de Selmer 0.

Prova. Denote por

$$x_0^F = \liminf_{n \rightarrow \infty} \frac{|\{E \in F; s_5(E) = 0, H(E) < n\}|}{|\{E \in F; H(E) < n\}|}$$

a proporção de curvas elípticas em F que possuem 5-posto de Selmer 0 (isto é, 5-grupo de Selmer trivial).

Como o *root number* é equidistribuído em F , pelo Teorema 5.1.14, a paridade de $s_5(E)$ é dada pela paridade de w_E , donde metade das curvas elípticas de F tem 5-posto de Selmer par e a outra metade ímpar. As que têm 5-posto de Selmer ímpar têm pelo menos 5 elementos do 5-grupo de Selmer. Pelo Teorema Dois, o tamanho médio dos 5-grupos de Selmer é 6. Logo,

$$x_0^F \cdot 5^0 + \left(\frac{1}{2} - x_0^F\right) \cdot 5^2 + \frac{1}{2} \cdot 5 \leq 6 \iff x_0^F \geq \frac{3}{8}. \quad \blacksquare$$

Em particular, se F é uma família com *root number* equidistribuído onde valem as hipóteses (i), (ii) e (iii) do Teorema Zero, $\frac{3}{8}$ de seus elementos satisfazem todas as condições do teorema e, portanto, satisfazem $r_{\text{alg}}(E) = r_{\text{an}}(E) = 0$.

Similarmente, o caso $s_p(E) = 1$:

Proposição 5.3.10. Seja F uma família de curvas elípticas com *root number* equidistribuído. Então, pelo menos $\frac{19}{40}$ das curvas elípticas em F , quando ordenadas por altura, têm 5-posto de Selmer 1.

Prova. Denote por

$$x_1^F = \liminf_{n \rightarrow \infty} \frac{|\{E \in F; s_5(E) = 1, H(E) < n\}|}{|\{E \in F; H(E) < n\}|}$$

a proporção de curvas elípticas que possuem 5-posto de Selmer 1 (isto é, 5-grupo de Selmer de ordem 5). Como na demonstração da Proposição 5.3.9, temos que

$$\frac{1}{2} \cdot 5^0 + x_1^F \cdot 5 + \left(\frac{1}{2} - x_1^F\right) \cdot 5^3 \leq 6 \iff x_1^F \geq \frac{19}{40}. \quad \blacksquare$$

Em particular, se F é uma família com *root number* equidistribuído onde valem as hipóteses (i), (ii), (iii), (iv) e (v) do Teorema Um, $\frac{19}{40}$ de seus elementos satisfazem todas as condições do teorema e, portanto, satisfazem $r_{\text{alg}}(E) = r_{\text{an}}(E) = 1$.

Mas ainda não usamos essa técnica em todo o seu potencial: note que, em quanto mais termos controláveis conseguirmos reduzir a soma ponderada das ordens dos p -grupos de

Selmer, menos informação perdemos. Isso nos motiva a tentar considerar os dois casos, 0 e 1, de uma só vez e, como se verá, isso é uma vantagem decisiva sobre os dois casos considerados separadamente: até mesmo se não pedimos equidistribuição do *root number*, conseguimos estimativas úteis!^[212]

Teorema 5.3.11. Seja F uma família de curvas elípticas. Então, $\frac{19}{24}$ das curvas elípticas em F têm 5-posto de Selmer 0 ou 1. Se o *root number* for equidistribuído em F , a cota melhora para $\frac{7}{8}$.

Prova. Seja

$$x_{0,1}^F = \liminf_{n \rightarrow \infty} \frac{|\{E \in F; s_5(E) \in \{0, 1\}, H(E) < n\}|}{|\{E \in F; H(E) < n\}|}$$

e, como antes, x_0^F para $s_5(E) = 0$ e x_1^F para $s_5(E) = 1$. Então, $1 - x_{0,1}^F$ das curvas elípticas de F têm 5-posto de Selmer pelo menos 2. Pelo Teorema Dois, o tamanho médio dos 5-grupos de Selmer é 6. Logo,

$$x_{0,1}^F + 5^2(1 - x_{0,1}^F) \leq 6 \iff x_{0,1}^F \geq \frac{19}{24}.$$

Esta cota é efetiva se para $\frac{19}{24}$ das curvas elípticas de F vale $s_5(E) = 0$ e para o restante, $s_5(E) = 2$.

Agora, suponha que o *root number* é equidistribuído em F . Como, pelo Teorema 5.1.14, a paridade se $s_5(E)$ é dada pela paridade de w_E , metade das curvas elípticas de F tem 5-posto de Selmer par e a outra metade ímpar. Assim,

$$x_0^F + 5x_1^F + 5^2 \left(\frac{1}{2} - x_0^F \right) + 5^3 \left(\frac{1}{2} - x_1^F \right) \leq 6 \iff 8x_0^F + 24x_1^F \geq 23.$$

Acrescentando a restrição $0 \leq x_1^F \leq \frac{1}{2}$ e minimizando $x_0^F + x_1^F$, obtemos

$$x_{0,1}^F \geq x_0^F + x_1^F \geq \frac{7}{8},$$

e este mínimo é alcançado se $\frac{3}{8}$ das curvas elípticas de F satisfazem $s_5(E) = 0$, $\frac{1}{2}$ satisfazem $s_5(E) = 1$, e o restante satisfaz $s_5(E) = 2$. ■

Em particular, se F é uma família onde valem as hipóteses (i), (ii) e (iii) do Teorema Zero e (i), (ii), (iii), (iv) e (v) do Teorema Um, $\frac{19}{24}$ de seus elementos satisfazem todas as condições de ambos os teoremas e, portanto, satisfazem $r_{\text{alg}}(E) = r_{\text{an}}(E) \in \{0, 1\}$. Se F , além disso, possui *root number* equidistribuído, esse valor sobre para incríveis $\frac{7}{8}$!

Observação 5.3.12. Recorde que, como acabamos de comentar, o p -posto de Selmer e o posto algébrico de uma curva elíptica estão relacionados. Mais especificamente, pela p -descida (Proposição 4.3.6), $s_p(E) = \log_p(\#\text{Sel}_p(E)) \geq r_{\text{alg}}(E)$. Logo, a ordem média do p -grupo de Selmer

^[212]Apenas para comparação, aquelas estimativas fracas que obtivemos sem pedir equidistribuição do *root number* no começo da seção eram, para $p = 5$, $x_0 \geq -\frac{1}{4}$ e $x_1 \leq \frac{5}{4}$, ou seja, absolutamente inúteis!

pode ser usada para encontrar uma cota superior para um “posto algébrico médio”, e é exatamente esta a técnica usada por Bhargava e Shankar para obter as cotas superiores para os posto algébrico médio (entendido a partir da ordem por altura) listadas na seção 5.1.3!

5.4 A maioria das curvas elípticas satisfaz BSD

Nesta seção, vamos impor as demais hipóteses dos Teoremas [Zero](#) e [Um](#), definindo famílias (que mostraremos serem grandes) onde estas condições são satisfeitas.

Definição 5.4.1. Seja $p \geq 5$. Definimos $S_0(p) \supseteq S'_1(p) \supseteq S_1(p)$ de modo que

- $S_0(p)$ é o conjunto das curvas elípticas que têm redução ordinária ou multiplicativa em p ;
- $S'_1(p)$ é o subconjunto de $S_0(p)$ formado pelas curvas elípticas E tais que, se E tem redução multiplicativa em p , $p \nmid v_p(\Delta(E))$. Além disso, se a redução for *split*, $v_p(\mathcal{L}_p(E)) = 1$;
- $S_1(p)$ é o subconjunto de $S'_1(p)$ que adiciona a condição: $\bar{\rho}_{E,p}$ ramifica em todo $\ell \equiv \pm 1 \pmod{p}$ tal que $v_\ell(N_E) = 1$.

Em suma, seus elementos satisfazem as seguintes propriedades:

	Teorema Zero			Teorema Um				
	(i)	(ii)	(iii)	(i)	(ii)	(iii)	(iv)	(v)
$S_0(p)$	×	×	*	×	×	*	×	*
$S'_1(p)$	×	×	*	×	×	*	×	*
$S_1(p)$	×	×	*	×	×	*	×	*

* = satisfeito por 100% das curvas elípticas sobre $\mathbb{Q}$ (Proposição 5.3.2).

Ficaram faltando os itens (iv) do Teorema [Zero](#) e (vi) do Teorema [Um](#), que dizem respeito ao p -grupo de Selmer. Como vimos na seção anterior, para termos à disposição o Teorema [Dois](#), precisamos nos especificar ao caso $p = 5$. Por isso, apesar de que todos os cálculos a seguir poder ser feitos para os outros primos, vamos nos deter apenas no caso que nos interessa.

Os próximos resultados tratam de mostrar que os conjuntos que definimos acima são, de fato, famílias grandes e de calcular (ou estimar) suas densidades. Para isto, interpretamos as condições sobre $E_{A,B}$ em termos de condições de congruência sobre os pares (A, B) , que podem ser mensuradas.

Proposição 5.4.2. $S_0(p)$ é uma família grande e $\mu(S_0(5)) = \frac{4 \cdot 5^{10}}{5(5^{10} - 1)} > 0,8$.

Prova. Pelo critério da Proposição 3.2.6, temos que $E_{A,B}$ tem redução boa ordinária em p se, e somente se, p não divide $\Delta(E_{A,B})$ nem o coeficiente de x^{p-1} em $(x^3 + Ax + B)^{(p-1)/2}$, que, para

$p = 5$, é $2A$. Além disso, por definição, $E_{A,B}$ tem redução má multiplicativa em p se, e somente se, $p \mid \Delta(E_{A,B})$ e $p \nmid A = -27c_4$. Em particular, estas são (finitas) condições de congruência módulo p , donde $S_0(p)$ é uma família grande.

Para $p = 5$, ambas as condições se reduzem a $5 \nmid A$. Logo,

$$\mu(S_0(5)) = \frac{4}{5} \cdot \left(1 - \frac{1}{5^{10}}\right)^{-1} = \frac{4 \cdot 5^{10}}{5(5^{10} - 1)} = 0,800000081920... > 0,8. \quad \blacksquare$$

Proposição 5.4.3. $S'_1(p)$ é uma família grande e

$$\mu(S'_1(5)) = \left(\frac{99}{125} - \frac{19}{125} \cdot \frac{4}{5^5 - 1}\right) \left(1 - \frac{1}{5^{10}}\right)^{-1} = 0,7918054...$$

Vimos na prova da proposição anterior o que significa, em termos de condições de congruência módulo p , a redução ser boa ordinária ou má multiplicativa. Agora, estabeleceremos um critério para saber quando uma redução multiplicativa é *split* que também pode ser interpretado como uma condição de congruência módulo p :

Lema 5.4.4. Suponha que $E_{A,B}$ tem redução multiplicativa em p . Então, a redução é *split* em p se, e somente se, $t^4 \equiv -3A \pmod{p}$ tem solução.

Prova. Como $E_{A,B}$ tem redução multiplicativa módulo p , $\bar{f}(x) = x^3 + \bar{A}x + \bar{B} \in \mathbb{F}_p[x]$ tem discriminante nulo. Logo, $\bar{f}$ tem uma raiz repetida x_0 , que também é uma raiz de $\bar{f}'(x) = 3x^2 + \bar{A} \implies 3x_0^2 = -\bar{A}$. Assim, $(x_0, 0)$ é a singularidade de $\tilde{E}_{A,B}$. Decompondo o termo homogêneo de menor grau nas retas tangentes a este ponto,

$$y^2 - x^3 - \bar{A}x - \bar{B} = (y - \alpha(x - x_0)) \cdot (y - \beta(x - x_0)) - (x - x_0)^3,$$

com $\alpha, \beta \in \overline{\mathbb{F}}_p$. Comparando os coeficientes em x , temos que $\alpha + \beta = 0$. Em particular, $\beta \in \mathbb{F}_p \iff \alpha \in \mathbb{F}_p$. Comparando os coeficientes em x^2 , temos que

$$2\alpha\beta x_0 + \underbrace{3x_0^2}_{=-\bar{A}} = \bar{A} \iff -\alpha^2 x_0 = \bar{A}.$$

Elevando ao quadrado e usando novamente que $3x_0^2 = -\bar{A}$, concluímos que $\alpha^4 = -3\bar{A}$. Logo, a equação $t^4 \equiv -3A \pmod{p}$ tem solução se, e somente se, $\alpha \in \mathbb{F}_p$, o que é equivalente a $E_{A,B}$ ter redução multiplicativa *split* em p . $\blacksquare$

Lema 5.4.5. Suponha que $E = E_{A,B}$ tem redução multiplicativa *split* em $p \geq 3$ e seja $k = v_p(\Delta(E))$. Se $p \nmid k$,

$$v_p(\mathcal{L}_p(E)) = 1 \iff \frac{\Delta(E)}{p^k} \pmod{p^2} \notin S_k \pmod{p^2},$$

onde $S_k \subseteq \mathbb{Z}_p^\times$ é dado por

$$S_k = \begin{cases} \{\omega - 24p\omega^2; \omega \in \mu_{p-1}\}, & \text{se } k = 1 \\ \mu_{p-1}, & \text{se } k > 1. \end{cases}$$

onde $\mu_{p-1} \subseteq \mathbb{Z}_p^\times$ é o conjunto das raízes $(p-1)$ -ésimas da unidade.

Prova. Seja q o período de Tate de E . Pela Proposição 1.5.4, podemos escrever $q = p^k \omega u$, com $k \in \mathbb{Z}$, $\omega \in \mu_{p-1}$ e $u \in 1 + p\mathbb{Z}_p$. Como vimos na seção 2.4, o discriminante de E se expressa em termos de q conforme a série de Fourier do discriminante modular (Exemplo 1.7.6):

$$\Delta(E) = q - 24q^2 + O(q^3) \implies \frac{\Delta(E)}{p^k} = \omega u - 24p^k \omega^2 u^2 + O(p^{2k}).$$

Assim,

$$\begin{aligned} u \equiv 1 \pmod{p^2} &\iff \frac{\Delta(E)}{p^k} \equiv \begin{cases} \omega \pmod{p^2}, & \text{se } k > 1 \\ \omega - 24p\omega^2 \pmod{p^2}, & \text{se } k = 1 \end{cases} \\ &\iff \frac{\Delta(E)}{p^k} \pmod{p^2} \in S_k \pmod{p^2}. \end{aligned}$$

Por outro lado,

$$\mathcal{L}_p(E) = \frac{\log_p(q)}{v_p(q)} = \frac{k \log_p(p) + \log_p(\omega) + \log_p(u)}{k}.$$

Como supomos que $p \nmid k$, $v_p(\mathcal{L}_p(E)) = v_p(\log_p(u))$. Logo, pela definição do logaritmo p -ádico,

$$v_p(\mathcal{L}_p(E)) = v_p(\log_p(u)) = 1 \iff u \notin 1 + p^2\mathbb{Z}_p \iff u \not\equiv 1 \pmod{p^2}. \quad \blacksquare$$

Prova da Proposição 5.4.3. Novamente, vamos interpretar a definição de $S'_1(p)$ em termos de condições de congruência módulo p .

- Como vimos na prova da Proposição 5.4.2, $E_{A,B} \in S'_1(p)$ tem redução boa ordinária em p se, e somente se, p não divide nem $\Delta(E_{A,B})$ nem o coeficiente de x^{p-1} em $(x^3 + Ax + B)^{(p-1)/2}$;
- $E_{A,B} \in S'_1(p)$ tem redução má multiplicativa em p se, e somente se, $p \mid \Delta(E_{A,B})$ e $p \nmid A$. Nesse caso, também pedimos que $p \nmid v_p(\Delta(E_{A,B}))$.

Além disso, pelo Lema 5.4.4, essa redução será *split* se, e somente se, $t^4 \equiv -3A \pmod{p}$ tem solução. Pelo Lema 5.4.5, a condição adicional $v_p(\mathcal{L}_p(E_{A,B})) = 1$ também se reduz a uma condição de congruência módulo p .

Logo, $S'_1(p) = F_{\Sigma_p}$ é uma família grande. Para $p = 5$, repartiremos Σ_5 nos seguintes subconjuntos disjuntos, que darão origem, respectivamente, aos elementos de $S'_1(p)$ que têm redução boa (ordinária), má multiplicativa não-*split* e *split*:

- Σ_5^{boa} é formado pelos pares $(A, B) \in \mathbb{Z}_5^2$ tais que 5 não divide A nem $\Delta(A, B)$. Note que, dados $a, b \in \mathbb{F}_5$, $\Delta(a, b) = \bar{0}$ se, e somente se, $a/3$ é um resíduo quadrático (duas opções, com duas raízes cada) ou $a = b = \bar{0}$. Como $\bar{A} \neq \bar{0}$, temos 20 cenários possíveis, dos quais 4 resultam em $\Delta(a, b) = \bar{0}$. Logo,

$$\mu_5(F_{\Sigma_5^{\text{boa}}}) = \frac{4}{5} \cdot \left(1 - \frac{4}{20}\right) \left(1 - \frac{1}{5^{10}}\right)^{-1} = \frac{16}{25} \left(1 - \frac{1}{5^{10}}\right)^{-1}.$$

- Σ_5^{nsplit} é formado pelos pares $(A, B) \in \mathbb{Z}_5^2$ tais que 5 divide $\Delta(A, B)$ mas não divide A nem $v_5(\Delta(A, B))$. Como $27B^2 \equiv -4A^3 \pmod{5}$ precisa ter solução, $A/3$ deve ser um resíduo quadrático (não nulo, nesse caso). Logo, $A \equiv 2$ ou $3 \pmod{5}$. Pelo Lema 5.4.4, como a redução é não-*split*, $t^4 \equiv -3A \pmod{5}$ não pode ter solução. Logo, $A \equiv 2 \pmod{5}$. Resta considerar que 5 não pode dividir $v_5(\Delta(A, B))$.

Seja $k > 0$, e tome uma classe para A módulo 5^{k+1} nas condições acima. Vale $v_5(\Delta(A, B)) = k$ se, e somente se, $27B^2 \equiv -4A^3 \pmod{5^k}$ tem solução e $27B^2 \equiv -4A^3 \pmod{5^{k+1}}$ não. Observe que as soluções da equação módulo 5^{k+1} também são soluções módulo 5^k . Logo, a estratégia é tomar as classes de B que resolvem a equação módulo 5^k (que são 2), estendê-las para classes módulo 5^{k+1} (que são $2 \cdot 5 = 10$) e retirar as classes que também resolvem a equação módulo 5^{k+1} (que são 2), resultando em 8 escolhas para B módulo 5^{k+1} que garantem as condições que procuramos. Assim, percorrendo k entre os inteiros tais que $5 \nmid k$ (a condição extra que pedimos para o caso de redução multiplicativa), obtemos

$$\mu_5(F_{\Sigma_5^{\text{nsplit}}}) = \left(1 - \frac{1}{5^{10}}\right)^{-1} \cdot \frac{1}{5} \cdot \sum_{\substack{k=1 \\ 5 \nmid k}}^{\infty} \frac{8}{5^{k+1}} = \frac{2}{25} \left(1 - \frac{4}{5^5 - 1}\right) \left(1 - \frac{1}{5^{10}}\right)^{-1}.$$

- Σ_5^{split} é formado pelos pares $(A, B) \in \mathbb{Z}_5^2$ tais que $A \equiv 3 \pmod{5}$ (consequência do Lema 5.4.4 e do item anterior). Como fizemos antes, incluiremos o resto das hipóteses nas possibilidades para B .

Como temos a restrição adicional caracterizada no Lema 5.4.5 para levar em conta, vamos usar a técnica de contagem do item anterior vendo as classes módulo 5^{k+2} em vez de 5^{k+1} (o motivo para isto é a condição sobre $\mathcal{L}_5$, como ficará claro logo adiante). Seja $k > 0$. Existem $2 \cdot 5^2 = 50$ classes módulo 5^{k+2} que resolvem a equação $27B^2 \equiv -4A^3 \pmod{5^k}$, das quais precisamos eliminar as $2 \cdot 5 = 10$ classes que também resolvem esta equação módulo 5^{k+1} . Até aqui, garantimos $v_5(\Delta(A, B)) = k$. Para garantir que $v_5(\mathcal{L}_5(E)) = 1$, precisamos eliminar as classes de B que garantem

$$\frac{\Delta(A, B)}{5^k} \pmod{5^2} \in S_k \pmod{5^2}.$$

No artigo (p. 9), afirma-se que são 4 as classes nestas condições (ver Nota 5.4.6). Como uma classe de B módulo 5^{k+2} que satisfaz esta propriedade não resolve a equação $27B^2 \equiv -4A^3 \pmod{5^{k+1}}$ (ou 5 dividiria $\frac{\Delta(E)}{5^k}$!), concluímos que 36 classes de B satisfazem as condições que queremos. Logo,

$$\mu_5(F_{\Sigma_5^{\text{split}}}) = \left(1 - \frac{1}{5^{10}}\right)^{-1} \cdot \frac{1}{5} \cdot \sum_{\substack{k=1 \\ 5 \nmid k}}^{\infty} \frac{36}{5^{k+2}} = \frac{9}{125} \left(1 - \frac{4}{5^5 - 1}\right) \left(1 - \frac{1}{5^{10}}\right)^{-1}.$$

Portanto, como $S'_1(5) = F_{\Sigma_5^{\text{boa}}} \cup F_{\Sigma_5^{\text{nsplit}}} \cup F_{\Sigma_5^{\text{split}}}$ é uma família definida apenas por condições de congruência módulo 5,

$$\begin{aligned} \mu(S'_1(5)) &= \mu_5(S'_1(5)) = \mu_5(F_{\Sigma_5^{\text{boa}}}) + \mu_5(F_{\Sigma_5^{\text{nsplit}}}) + \mu_5(F_{\Sigma_5^{\text{split}}}) \\ &= \left(\frac{99}{125} - \frac{19}{125} \cdot \frac{4}{5^5 - 1} \right) \left(1 - \frac{1}{5^{10}} \right)^{-1} = 0,7918054... \quad \blacksquare \end{aligned}$$

Nota 5.4.6. Aparentemente, houve um pequeno equívoco na contagem das opções para B dentro do cálculo da densidade de Σ_5^{split} na prova acima. Afirma-se no artigo que, como escrevemos, são 4 as classes para B módulo 5^{k+2} que, nas condições anteriores (isto é, $A \equiv 3 \pmod{5}$ e $v_5(\Delta(A, B)) = k > 0$), satisfazem

$$\frac{\Delta(A, B)}{5^k} \pmod{5^2} \in S_k \pmod{5^2}$$

Argumentamos que são 8 as classes nestas condições.

Comece notando que $\#S_k = 4$ para todo k : para $k = 1$, basta ver que os 4 elementos da forma $\omega - 24p\omega^2$ têm resíduos distintos módulo $p = 5$.

Escreva $\Delta(A, B) = 5^k(x + 5^2y) \iff \frac{\Delta(A, B)}{5^k} = x + 5^2y$. Logo,

$$\begin{aligned} x \pmod{5^2} \in S_k &\iff 5^k \cdot x \in 5^k \cdot S_k \pmod{5^{k+2}} \\ \iff \frac{\Delta(A, B)}{5^k} \pmod{5^2} \in S_k \pmod{5^2} &\iff \Delta(A, B) \pmod{5^{k+2}} \in 5^k \cdot S_k \pmod{5^{k+2}} \end{aligned}$$

Assim, $B^2 \pmod{5^{k+2}} \in \tilde{S}_k \doteq \left\{ \frac{5^k \cdot x}{27} - 4 \left(\frac{A}{3} \right)^3, x \in S_k \right\} \pmod{5^{k+2}}$. Para todo $\tilde{x} \in \tilde{S}_k$, $\tilde{x} \not\equiv 0 \pmod{5}$. Logo, como

a é quadrado em $(\mathbb{Z}/p^n\mathbb{Z})^\times$ se, e somente se, a é quadrado em $(\mathbb{Z}/p\mathbb{Z})^\times$ ^[213]

e $\frac{5^k \cdot x}{27} - 4 \left(\frac{A}{3} \right)^3 \equiv -4 \left(\frac{A}{3} \right)^3 \equiv 1 \pmod{5}$, todos os $\# \tilde{S}_k = 4$ são quadrados módulo 5^{k+2} . Assim, existem 8 classes de B módulo 5^{k+2} , a saber, as raízes de cada elemento de $\tilde{S}_k$ nas condições do enunciado ^[214], concluindo a prova.

Isto faz com que o valor de $\mu(S'_1(5))$ caia ligeiramente, influenciando também, ainda que pouco, os resultados seguintes:

$$\mu(S'_1(5)) = \left(\frac{98}{125} - \frac{18}{125} \cdot \frac{4}{5^5 - 1} \right) \left(1 - \frac{1}{5^{10}} \right)^{-1} = 0,7838157...$$

Proposição 5.4.7. $S_1(p)$ é uma família grande e $\mu(S_1(5)) > 0,7917957$.

^[213]Para a ida, basta usar o Lema de Hensel com o polinômio $x^2 - a$. A volta é trivial.

^[214]Pois $(\mathbb{Z}/5^{k+2}\mathbb{Z})^\times$ é cíclico.

Prova. Sejam $E = E_{A,B}$ e $\ell \equiv \pm 1 \pmod{p}$ tal que $v_\ell(N_E) = 1$, ou seja, E tem redução multiplicativa em ℓ . Pela Proposição 3.4.8, $\bar{\rho}_{E,p}$ ramifica em ℓ se, e somente se, $p \nmid v_\ell(\Delta(E))$.

Como, para cada $\ell \equiv \pm 1 \pmod{p}$, cada $\Sigma_\ell \doteq \{(A,B); \ell \mid N(E_{A,B}) \implies p \nmid v_\ell(\Delta(E_{A,B}))\}$ são finitas condições de congruência módulo ℓ , cada F_{Σ_ℓ} é uma família grande e, pela definição, verifica-se que $S_1(p) = S'_1(p) \cap \bigcap_{\ell \equiv \pm 1 \pmod{p}} F_{\Sigma_\ell}$, $S_1(p)$ também é uma família grande^[215]. Seja $p = 5$. Temos que

$$\mu(S_1(5)) = \mu\left(S'_1(5) \cap \bigcap_{\ell \equiv \pm 1 \pmod{5}} F_{\Sigma_\ell}\right) = \mu(S'_1(5)) \prod_{\ell \equiv \pm 1 \pmod{5}} \mu_\ell(F_{\Sigma_\ell}).$$

Vamos estimar os fatores do produto. Trocando, em cada Σ_ℓ , a condição $\ell \mid N(E_{A,B}) \implies p \nmid v_\ell(\Delta(E_{A,B}))$ por $\ell \mid \Delta(A,B) \implies p \nmid v_\ell(\Delta(E_{A,B}))$, estamos abrandando “a restrição sobre a restrição” e, portanto, potencialmente aumentando o número de restrições sobre (A,B) . Assim, $\mu_\ell(F_{\Sigma_\ell}) \geq \mu_\ell(F_{\Sigma'_\ell})$, onde Σ'_ℓ é o conjunto dado pelas novas restrições.

Calculemos $\mu_\ell(F_{\Sigma'_\ell})$. Note que

$$\mu_\ell(\Sigma'_\ell) = 1 - \mu_\ell(\{(A,B) \in \mathbb{Z}_5^2; \ell \mid \Delta(A,B) \text{ e } 5 \mid v_\ell(\Delta(A,B))\}).$$

Calcularemos esta densidade dividindo em dois casos (disjuntos): $\ell \mid A$ e $\ell \nmid A$:

- $\ell \mid A$: Nesse caso, como $5 \mid v_\ell(\Delta(A,B)) > 0$, é fácil ver que $\ell^2 \mid A$ e $\ell^3 \mid B$. Logo, a densidade deste subconjunto é $\frac{1}{\ell^5}$;
- $\ell \nmid A$: Estamos nas condições do Lema 5.3.4, que nós dá que a densidade deste subconjunto é

$$\sum_{\substack{k=1 \\ 5 \nmid k}}^{\infty} \frac{\ell-1}{\ell} \cdot \frac{2(\ell-1)}{\ell^{k+1}} = \sum_{\substack{k=1 \\ 5 \nmid k}}^{\infty} \frac{(\ell-1)^2}{\ell^{k+2}} = \left(1 - \frac{1}{\ell}\right)^2 \frac{1}{\ell^5 - 1}.$$

Logo,

$$\mu(S_1(5)) \geq \mu(S'_1(5)) \cdot \prod_{\ell \equiv \pm 1 \pmod{5}} \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \left(1 - \frac{1}{\ell}\right)^2 \frac{1}{\ell^5 - 1} - \frac{1}{\ell^5}\right).$$

Observe que os fatores do produto (infinito) convergem para 1 (por baixo) muito rapidamente. Calculando os 5 primeiros termos ($\ell \in \{11, 19, 29, 31, 41\}$), obtemos a cota inferior 0,7917957... para este produto. ■

Corolário 5.4.8. $\mu(S'_1(5)) - \mu(S_1(5)) \leq 0,00001$.

^[215]Observe que esta intersecção é infinita, pelo Teorema de Dirichlet sobre primos em progressões aritméticas (SERRE, 1973, p. 25, Lema 3), e que intersecção infinita de famílias grandes pode não ser uma família grande. Por isso é que temos que recorrer à definição.

Nota 5.4.9. A alteração descrita na Nota 5.4.6 influencia a densidade de $\mu(S_1(5))$ também. Porém, antes propomos uma melhoria para este resultado: afirmamos que o caso $\ell \mid A$ considerado na prova da Proposição 5.4.7 simplesmente não ocorre, ou, mais especificamente,

$$\mu(S_1(5)) = \mu(S'_1(5)) \cdot \prod_{\ell \equiv \pm 1 \pmod{p}} \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \left(1 - \frac{1}{\ell}\right)^2 \frac{1}{\ell^5 - 1}\right).$$

Para ver isto, observe que $S_1(p)$ é o subconjunto de $S'_1(p)$ onde se adiciona a condição

$$E \in S_1(p) \text{ se para todo } \ell \equiv \pm 1 \pmod{p} \text{ tal que } v_\ell(N_E) = 1, \bar{\rho}_{E,p} \text{ ramifica em } \ell.$$

Como, E é ℓ -integral, $v_\ell(N_E) = 1$ é equivalente a E ter redução multiplicativa em ℓ , que é equivalente a $\ell \mid \Delta(E)$ e $\ell \nmid A$. Além disso, como a redução é multiplicativa em ℓ , pela Proposição 3.4.8, $\bar{\rho}_{E,p}$ ramifica em ℓ é equivalente a $p \nmid v_\ell(\Delta(E))$. Logo, podemos reescrevê-la como

$$E \in S_1(p) \text{ se, para todo } \ell \equiv \pm 1 \pmod{p}, \ell \mid \Delta(E) \text{ e } \ell \nmid A \implies p \nmid v_\ell(\Delta(E)).$$

Assim, $S_1(p) = S'_1(p) \cap \bigcap_{\ell \equiv \pm 1 \pmod{p}} F_{\Sigma_\ell}$, onde

$$\Sigma_\ell = \{(A, B) \in \mathbb{Z}_p^2, \ell \mid \Delta(A, B) \text{ e } \ell \nmid A \implies p \nmid v_\ell(\Delta(A, B))\}.$$

Como antes, cada F_{Σ_ℓ} é definida por finitas condições de congruência e, portanto, é família grande. $S_1(p)$ também é uma família grande, pela definição. Calculemos sua densidade para $p = 5$. Temos que

$$\begin{aligned} \mu(S_1(5)) &= \mu(S'_1(5)) \cdot \mu\left(\bigcap_{\ell \equiv \pm 1 \pmod{p}} F_{\Sigma_\ell}\right) \\ &= \mu(S'_1(5)) \cdot \prod_{\ell \text{ primo}} \mu\left(\bigcap_{\ell \equiv \pm 1 \pmod{p}} F_{\Sigma_\ell}\right) \\ &= \mu(S'_1(5)) \cdot \prod_{\ell \equiv \pm 1 \pmod{p}} \mu_\ell(F_{\Sigma_\ell}) = \mu(S'_1(5)) \cdot \prod_{\ell \equiv \pm 1 \pmod{p}} \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \mu_\ell(\Sigma_\ell) \end{aligned} \tag{5.1.7}$$

Para concluir, resta calcular $\mu_\ell(\Sigma_\ell)$. Como a condição que define Σ_ℓ é de implicação, é mais fácil considerar o complementar:

$$\mu_\ell(\Sigma_\ell) = 1 - \mu_\ell(\{(A, B) \in \mathbb{Z}_p^2, \ell \mid \Delta(A, B), \ell \nmid A \text{ e } p \mid v_\ell(\Delta(A, B))\}).$$

As duas primeiras restrições nos colocam nas condições do Lema 5.1.18, que nos dá que

$$\mu_\ell(\Sigma_\ell) = 1 - \sum_{\substack{k=1 \\ 5 \nmid k}}^{\infty} \frac{(\ell-1)^2}{\ell^{k+2}} = 1 - \left(1 - \frac{1}{\ell}\right)^2 \frac{1}{\ell^5 - 1},$$

concluindo a prova.

Em vista destas considerações e da Nota 5.4.6, obtemos que

$$\mu(S_1(5)) \geq 0,7838113... \quad \text{e} \quad \mu(S'_1(5)) - \mu(S_1(5)) \leq 0,0000044,$$

que, por um lado, é uma leve queda na Proposição 5.4.7, mas, por outro lado, nos dá uma grande melhoria no Corolário 5.4.8.

Agora, lidamos com as hipóteses dos Teoremas Zero e Um relacionadas ao 5-grupo de Selmer. Para isto, como vimos na seção anterior, precisamos de famílias com *root number* equidistribuído onde valem as demais condições de cada teorema. Infelizmente, não temos nenhuma informação sobre a distribuição do *root number* nas famílias que acabamos de estudar, mas o Corolário 5.1.17 nos lembra que em cada uma delas, há uma subfamília com *root number* equidistribuído^[216].

Proposição 5.4.10. Quando ordenadas por altura, pelo menos 16,50% das curvas elípticas sobre $\mathbb{Q}$ têm posto algébrico e analítico 0.

Prova. Pelo Corolário 5.1.17, $S_0(5)$ tem uma subfamília F de densidade $\mu(F) \geq 0,5501 \cdot \mu(S_0(5))$ onde o *root number* é equidistribuído. Pela Proposição 5.3.9, $\frac{3}{8}$ das curvas elípticas de F têm p -grupo de Selmer trivial donde, pelo Teorema Zero, têm posto algébrico e analítico 0. Logo, pelo menos

$$\mu(F) \cdot \frac{3}{8} \geq 0,5501 \cdot \mu(S_0(5)) \cdot \frac{3}{8} = 0,16503,$$

isto é, 16,50% das curvas elípticas sobre $\mathbb{Q}$ têm posto algébrico e analítico 0. ■

Proposição 5.4.11. Quando ordenadas por altura, pelo menos 20,68% das curvas elípticas sobre $\mathbb{Q}$ têm posto algébrico e analítico 1.

Prova. Pelo Corolário 5.1.17, $S_1(5)$ tem uma subfamília F de densidade $\mu(F) \geq 0,5501 \cdot \mu(S_1(5))$ onde o *root number* é equidistribuído. Pela Proposição 5.3.10, $\frac{19}{40}$ das curvas elípticas de F têm p -posto de Selmer 1 donde, pelo Teorema Um, têm posto algébrico e analítico 1. Logo, pelo menos

$$\mu(F) \cdot \frac{19}{40} \geq 0,5501 \cdot \mu(S'_1(5)) \cdot \frac{19}{40} - 0,00001 \geq 0,20688,$$

isto é, 20,68% das curvas elípticas sobre $\mathbb{Q}$ têm posto algébrico e analítico 1. ■

Até aqui, pelo menos 37,18% das curvas elípticas satisfazem BSD. Porém, como vimos na seção anterior, essa técnica de contagem é bem mais forte se consideramos os dois casos de uma só vez:

^[216]Não necessariamente grande e nem definida por condições de congruência, é bom lembrar.

Teorema 5.4.12. Quando ordenadas por altura, pelo menos 66,48% das curvas elípticas sobre $\mathbb{Q}$ têm posto algébrico e analítico 0 ou 1.

Prova. Como nos casos anteriores, quanto mais curvas elípticas de $S_1(5)$ soubermos ter *root number* equidistribuído, melhor. Sabemos pelo Corolário 5.1.17 que $S_1(5)$ tem uma subfamília F de densidade $\mu(F) \geq \kappa \cdot \mu(S_1(5))$, com $\kappa > 0,5501$, onde o *root number* é equidistribuído. Pelo Corolário 5.4.8, $\mu(F) \geq \kappa\mu(S'_1(5)) - 0,00001$. Pelo Teorema 5.3.11, $\frac{7}{8}$ das curvas elípticas de $F \subseteq S_1(5)$ satisfazem todas as condições dos Teoremas Zero ou Um e, portanto, têm posto algébrico e analítico 0 ou 1. Até agora, nossa cota é de

$$\frac{7}{8}\mu(F) \geq \frac{7}{8}(\kappa\mu(S'_1(5)) - 0,00001) \geq 38,11\%^{[217]}$$

Apesar de não termos informação sobre a distribuição do *root number* no complementar de F , ainda podemos considerá-lo (toda ajuda para aumentar a cota é bem-vinda, afinal). Como F é dado por uma união finita de subfamílias de $S_1(5)$, seu complementar é uma união possivelmente infinita de subfamílias grandes de $S_1(5)$, o que não necessariamente é uma família grande. Porém, podemos aproximar $S_1(5) - F$ por famílias grandes F'_ε de modo que, para cada $\varepsilon > 0$,

$$\mu(F'_\varepsilon) \geq \mu(S_1(5)) - \mu(F) - \varepsilon \geq (1 - \kappa)\mu(S'_1(5)) - 0,00001 - \varepsilon.$$

Pelo Teorema 5.3.11, pelo menos $\frac{19}{24}$ das curvas elípticas em $F'_\varepsilon \subseteq S_1(5)$ satisfazem todas as condições dos Teoremas Zero ou Um e, portanto, têm posto algébrico e analítico 0 ou 1. Logo, das curvas elípticas em $S_1(5)$, tanto em F quanto no complementar, sabemos que pelo menos

$$\left(\frac{7}{8}\kappa + \frac{19}{24}(1 - \kappa)\right) \cdot \mu(S'_1(5)) - \left(\frac{7}{8} + \frac{19}{24}\right) \cdot 0,00001 \geq 0,663126$$

das curvas elípticas sobre $\mathbb{Q}$ têm posto algébrico e analítico 0 ou 1.

Já tiramos tudo o que podíamos de $S_1(5)$. Ainda podemos olhar para o restante das curvas elípticas em $S_0(5)$, que ainda podem satisfazer o Teorema Zero. Pelo Corolário 5.1.17, $S_0(5)$ possui uma subfamília $F^{[218]}$ de densidade $\mu(F) \geq \kappa \cdot \mu(S_0(5))$, com $\kappa > 0,5501$, onde o *root number* é equidistribuído. Pela Proposição 5.3.9, pelo menos $\frac{3}{8}$ das curvas elípticas em $F \cap (S_0(5) - S_1(5))$ satisfazem todas as condições do Teorema Zero e, portanto, têm posto algébrico e analítico 0, acrescentando mais

$$\frac{3}{8} \cdot \kappa \cdot \mu(S_0(5)) - \mu(S'_1(5)) \geq 0,00169$$

à cota inferior, totalizando 66,4816%. ■

^[217]Já é mais do que o que se obteve antes ao considerar os dois casos separadamente!

^[218]Usamos a mesma letra intencionalmente, já que a intersecção desta subfamília com $S_1(5)$ coincide, por construção, com a subfamília $F \subseteq S_1(5)$ considerada anteriormente.

Conclusão da Prova do Teorema BSZ. Do Teorema 5.4.12, já obtemos que pelo menos 66,48% das curvas elípticas, quando ordenadas por altura, satisfazem $r_{\text{an}}(E) = r_{\text{alg}}(E) \leq 1$. Para finalizar, basta invocar o Teorema de Kolyvagin–Rubin (Teorema 4.3.17) para obter que, para tais curvas elípticas, $r_{\text{an}}(E) \leq 1 \implies \#\text{III}(E) < \infty$. ■

Nota 5.4.13. Em vista da Nota 5.4.9, a margem de erro descrita no Corolário 5.4.8 se torna irrelevante para a precisão de casas decimais que estamos utilizando, sumindo com todas as margens de erro nas contas acima. Por outro lado, temos que levar em conta a correção do valor de $\mu(S'_1(5))$ descrita na Nota 5.4.6. No final, a proporção corrigida de curvas elípticas sobre $\mathbb{Q}$ que satisfazem $r_{\text{alg}}(E) = r_{\text{an}}(E) \leq 1$ é 65,979%, uma redução de cerca de 0,5%.

5.4.1 Quanto é “a maioria”?

Apesar desta já ser uma quantidade considerável de curvas elípticas para as quais se tem certeza da validade da conjectura, este valor pode ser aprimorado se os teoremas utilizados para obtê-lo pudessem ser fortalecidos pela retirada de hipóteses ou pela extensão dos mesmos para curvas elípticas com outros tipos de reduções (os autores do artigo estimam que, feitas todas as melhorias que indicam, esta cota inferior poderia subir para mais de 80% (BHARGAVA; SKINNER; ZHANG, 2014, p. 14).

Isto tudo, ainda, trabalhando apenas com os (pouquíssimos) casos em que sabemos que vale a Conjectura de Bhargava. Se esta conjectura for verificada, a “maioria” se torna 100% das curvas elípticas!^[219]

Teorema 5.4.14 (Bhargava–Skinner–Zhang). Se a Conjectura de Bhargava for verdadeira^[220], então 100% das curvas elípticas têm posto 0 ou 1. Em particular, 100% das curvas elípticas satisfazem a Conjectura de Birch e Swinnerton-Dyer^[221].

Demonstração. Pela prova do Teorema 5.3.11, pelo menos $\frac{p^2 - p - 1}{p^2 - 1}$ das curvas elípticas em $S_1(p)$ têm posto 0 ou 1. Além disso,

$$\mu(S_1(p)) \geq \left(1 - \frac{1}{p^{10}}\right)^{-1} \cdot \left(1 - \frac{1}{p}\right)^2 \cdot \underbrace{\prod_{\ell \equiv \pm 1 \pmod{p}} \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \frac{1}{\ell^5}\right)^2}_{\doteq \Pi_p}.$$

^[219] Isto, é claro, não prova a Conjectura BSD para *todas* as curvas elípticas, mas já traz resultados interessantes (além de bastante esperança para a validade da própria conjectura BSD!): por exemplo, $X\%$ das curvas elípticas têm posto 0, $Y\%$ das curvas elípticas têm posto 1 e 0% das curvas elípticas têm posto maior que 1 se, e somente se, o posto algébrico médio das curvas elípticas é $\frac{Y}{X+Y}$. Em particular, se a Conjectura de Bhargava for verdadeira, a Conjectura de Goldfeld–Katz–Sarnak (Conjectura 5.1.19) é equivalente à conjectura “folclórica” de que o posto algébrico médio das curvas elípticas é $\frac{1}{2}$ (Conjectura 5.1.18)!

^[220] Na verdade, basta que a conjectura valha para uma sequência de primos.

^[221] E a de Tate–Shafarevich (Conjectura 4.3.16)!

Para ver isto, adaptando a prova da Proposição 5.4.7 temos que

$$\mu(S_1(p)) \geq \mu(S'_1(p)) \cdot \prod_{\ell \equiv \pm 1 \pmod p} \left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \frac{(\ell-1)^2}{\ell^2(\ell^p-1)} - \frac{1}{\ell^5}\right). \quad [222]$$

O primeiro termo pode ser estimado como na prova da Proposição 5.4.3 levando em conta apenas a subfamília das curvas elípticas de redução boa, obtendo os dois primeiros fatores do produto anterior e, para os termos de Π_p , basta usar técnicas de cálculo diferencial para ver que

$$1 - \frac{(\ell-1)^2}{\ell^2(\ell^p-1)} - \frac{1}{\ell^5} \geq \left(1 - \frac{1}{\ell^5}\right)^2$$

para todo p primo [223].

Logo,

$$\lim_{p \rightarrow \infty} \frac{p^2 - p - 1}{p^2 - 1} \cdot \mu(S_1(p)) \geq \lim_{p \rightarrow \infty} \frac{p^2 - p - 1}{p^2 - 1} \cdot \left(1 - \frac{1}{p^{10}}\right)^{-1} \cdot \left(1 - \frac{1}{p}\right)^2 \cdot \Pi_p.$$

É fácil ver que os três primeiros termos do produto acima convergem para 1. Lidamos com o produto infinito Π_p transformando numa soma infinita. Considere a série

$$\Sigma_p \doteq \sum_{\ell \equiv \pm 1 \pmod p} \log \left(1 - \frac{2}{\ell^5 + 1}\right),$$

que se convergir, é $\log(\Pi_p)$ [224]. Como $\log(1+x) \leq x$ para $x \geq -1$ e a série $\sum_{\ell \equiv \pm 1 \pmod p} \frac{2}{\ell^5 + 1}$ converge uniformemente, Σ_p converge uniformemente. Seja p_j o j -ésimo primo depois do 5 ($p_0 = 5$), seja $(\ell_{ij})_i$ a sequência crescente dos primos que satisfazem $\ell_{ij} \equiv \pm 1 \pmod{p_j}$ e denote

$$a_{ij} = \frac{\ell_{ij}^5 - 1}{\ell_{ij}^5 + 1}.$$

Como $\ell_{ij} \geq p_j$ para todo i , $\lim_{j \rightarrow \infty} a_{ij} = 1$ para todo i . Logo,

$$\begin{aligned} \log(\lim_{p \rightarrow \infty} \Pi_p) &= \lim_{p \rightarrow \infty} \log(\Pi_p) = \lim_{p \rightarrow \infty} \Sigma_p = \lim_{j \rightarrow \infty} \sum_{i=1}^{\infty} \log(a_{ij}) \stackrel{[225]}{=} \sum_{i=1}^{\infty} \underbrace{\log\left(\lim_{j \rightarrow \infty} a_{ij}\right)}_{=1} = 0 \\ \implies \lim_{p \rightarrow \infty} \Pi_p &= \exp(0) = 1. \end{aligned}$$

Logo, $\lim_{p \rightarrow \infty} \frac{p^2 - p - 1}{p^2 - 1} \cdot \mu(S_1(p)) \geq 1$, donde 100% das curvas elípticas sobre $\mathbb{Q}$ possuem posto algébrico e analítico 0 ou 1. Em particular, 100% das curvas elípticas sobre $\mathbb{Q}$ satisfazem a Conjectura de Birch e Swinnerton-Dyer. ■

[222] Sim, é $\frac{1}{\ell^5}$ mesmo, pois corresponde à densidade do conjunto dos (A, B) tais que $\ell^2 \mid A$ e $\ell^3 \mid B$.

[223] Este argumento também funciona com a modificação que propusemos na Nota 5.4.9.

[224] Note que $\left(1 - \frac{1}{\ell^{10}}\right)^{-1} \left(1 - \frac{1}{\ell^5}\right)^2 = \frac{\ell^5 - 1}{\ell^5 + 1} = 1 - \frac{2}{\ell^5 + 1}$.

[225] A inversão dos limites está justificada pela convergência uniforme discutida acima.

REFERÊNCIAS

AHLFORS, L. **Complex Analysis**: An introduction to the theory of analytic functions of one complex variable. 3rd. ed. Nova Iorque: McGraw-Hill, 1979. Citado na página 69.

AITKEN, W.; LEMMERMEYER, F. **Counterexamples to the Hasse Principle**. 2011. Disponível em: <<https://arxiv.org/abs/1108.6310>>. Citado na página 101.

APOSTOL, T. M. **Introduction to Analytic Number Theory**. Nova Iorque: Springer, 1976. (Undergraduate Texts in Mathematics). Citado nas páginas 53 e 54.

ASH, A.; GROSS, R. **Elliptic Tales**: Curves, counting and number theory. Princeton: Princeton University Press, 2012. Nenhuma citação no texto.

ATIYAH, M. F.; MACDONALD, I. G. **Introduction to Commutative Algebra**. Reading, MA: Addison-Wesley Publishing Company, 1969. Citado na página 109.

AURICHI, L. **Notas de Aula (Topologia)**. 2017. Disponível em: <<http://conteudo.icmc.usp.br/pessoas/aurichi/lib/exe/fetch.php?media=curso:topologia2017.pdf>>. Citado nas páginas 30, 109 e 111.

BEKTEMIROV, B.; MAZUR, B.; STEIN, W.; WATKINS, M. Average ranks of elliptic curves: tension between data and conjecture. **Bull. Amer. Math. Soc. (N.S.)**, v. 44, n. 2, p. 233–254, 2007. Citado na página 123.

BERTOLINI, M.; DARMON, H. **The p -adic L -functions of modular elliptic curves**. 2007. Disponível em: <<http://www.math.mcgill.ca/darmon/pub/Articles/Research/29.Millennium/paper.pdf>>. Citado nas páginas 76 e 106.

BHARGAVA, M. **The average rank of elliptic curves**. 2011. Conference on the BSD Conjecture at DPPM, Cambridge Univ. Disponível em: <<https://www.dpmms.cam.ac.uk/research/BSD2011/bsd2011-Bhargava.pdf>>. Nenhuma citação no texto.

_____. A positive proportion of plane cubics fail the Hasse principle. 2014. Disponível em: <<https://arxiv.org/pdf/1402.1131.pdf>>. Citado na página 101.

BHARGAVA, M.; KANE, D. M.; LENSTRA JR., H. W.; POONEN, B.; RAINS, E. **Modeling the distribution of ranks, Selmer groups and Shafarevich–Tate groups of elliptic curves**. 2013. Disponível em: <<https://arxiv.org/abs/1304.3971>>. Citado na página 109.

BHARGAVA, M.; SHANKAR, A. The average number of elements in the 4-Selmer groups of elliptic curves is 7. 2013. Disponível em: <<https://arxiv.org/abs/1312.7333>>. Citado na página 130.

_____. **The average size of the 5-Selmer group of elliptic curves is 6, and the average rank of elliptic curves is less than 1**. 2013. Disponível em: <<https://arxiv.org/abs/1312.7859>>. Citado nas páginas 121, 122 e 130.

_____. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. 2013. Disponível em: <<https://arxiv.org/abs/1006.1002>>. Citado nas páginas 119, 122 e 130.

_____. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. 2013. Disponível em: <<https://arxiv.org/abs/1007.0052>>. Citado nas páginas 122 e 130.

BHARGAVA, M.; SKINNER, C. A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one. **J. Ramanujan Math. Soc.**, v. 29, n. 2, 2013. Disponível em: <<https://arxiv.org/abs/1401.0233>>. Nenhuma citação no texto.

BHARGAVA, M.; SKINNER, C.; ZHANG, W. **A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture**. 2014. Disponível em: <<https://arxiv.org/abs/1407.1826>>. Citado nas páginas 11, 13, 20, 116, 127 e 142.

BIRCH, B.; SWINNERTON-DYER, P. Notes on elliptic curves (II). **J. Reine Angew. Math.**, v. 165, n. 218, p. 79–108, 1965. Citado na página 85.

BOMBIERI, E. **Problems of the Millennium: the Riemann Hypothesis**. 2000. Disponível em: <https://www.claymath.org/sites/default/files/sarnak_rh_0.pdf>. Citado na página 53.

BOREVICH, Z. I.; SHAFAREVICH, I. R. **Number Theory**. Nova Iorque: Academic Press, 1966. Citado na página 46.

BORGES, H.; TENGAN, E. **Álgebra Comutativa em Quatro Movimentos**. Rio de Janeiro: IMPA, 2015. Citado nas páginas 23, 37 e 109.

BRADY, Z. E. **Weil stuff**. 2017. Disponível em: <<https://math.mit.edu/~notzeb/weil.pdf>>. Citado na página 30.

BREUIL, C.; CONRAD, B.; DIAMOND, F.; TAYLOR, R. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. **J. Amer. Math. Soc.**, v. 14, n. 4, p. 843–939, 2001. Citado nas páginas 19 e 82.

BRUIN, P. **What is... an L-function?** 2012. Disponível em: <<https://www.math.leidenuniv.nl/~pbruin/L-functions.pdf>>. Citado na página 53.

BRUINIER, J. H.; GEER, G. van der; HARDER, G.; ZAGIER, D. **The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway**. Berlim: Springer, 2008. Citado na página 49.

BRUMER, A. The average rank of elliptic curves I. **Inv. Math.**, v. 109, p. 445–472, 1992. Citado nas páginas 118 e 122.

BUHLER, J. P.; GROSS, B. H.; ZAGIER, D. B. On the Conjecture of Birch and Swinnerton-Dyer for an Elliptic Curve of Rank 3. **Math. of Comp.**, v. 44, n. 170, p. 473–481, 1985. Citado na página 162.

CASSELS, J. W. S. Arithmetic on curves of genus 1. III. Tate-Šafarevič and Selmer groups. **Proc. London Math. Soc.**, v. 12, n. 3, p. 259–296, 1962. Citado na página 106.

_____. **Lectures on Elliptic Curves**. Cambridge: Cambridge University Press, 1991. (London Mathematical Society Student Texts, 24). Nenhuma citação no texto.

- CIPRA, B. Math as She is Wrote. In: OLIVEIRA, M. P. S. de (Ed.). **Teias Matemáticas**. Coimbra: Imprensa da Universidade de Coimbra, 2004. p. 13–24. Citado na página 93.
- COATES, J.; WILES, A. On the conjecture of Birch and Swinnerton-Dyer. **Inv. Math.**, v. 39, n. 3, p. 223–251, 1977. Citado nas páginas 20 e 85.
- COHEN, H. **A Course in Computational Algebraic Number Theory**. Berlim: Springer, 1996. (Graduate Texts in Mathematics, 138). Citado na página 160.
- CONRAD, K. **Ostrowski for Number Fields**. Disponível em: <<https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf>>. Nenhuma citação no texto.
- _____. **The Congruent Number Problem**. 2019. Disponível em: <<https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf>>. Citado na página 163.
- _____. **Cyclicity of $(\mathbb{Z}/(p))^{\times}$** . 2019. Disponível em: <<https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf>>. Citado na página 81.
- _____. **Examples of Mordell’s Equation**. 2019. Disponível em: <<https://kconrad.math.uconn.edu/blurbs/gradnumthy/mordelleqn1.pdf>>. Citado na página 77.
- _____. **Modules over a PID**. 2019. Disponível em: <<https://kconrad.math.uconn.edu/blurbs/linmultialg/modulesoverPID.pdf>>. Nenhuma citação no texto.
- CORNELL, G.; SILVERMAN, J. H.; STEVENS, G. (Ed.). **Modular Forms and Fermat’s Last Theorem**. Nova Iorque: Springer, 1997. Citado na página 82.
- CREMONA, J. E. **Algorithms for Modular Elliptic Curves**. 2a. ed. Cambridge: Cambridge University Press, 1997. Citado nas páginas 83 e 88.
- _____. **Numerical evidence for the Birch–Swinnerton-Dyer conjecture**. 2011. Slides de Palestra na Conferência BSD (Cambridge, 2011). Disponível em: <<https://people.maths.bris.ac.uk/~matyd/BS2011/bsd2011-Cremona.pdf>>. Citado na página 162.
- _____. **Elliptic Curve Data**. 2019. Banco de dados de curvas elípticas sobre $\mathbb{Q}$. Disponível em: <<http://johncremona.github.io/ecdata/>>. Citado na página 87.
- _____. **eclib (including mwrank and related programs for elliptic curves over $\mathbb{Q}$)**. 2019. Disponível em: <<http://homepages.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html>>. Citado na página 87.
- DARMON, H.; DIAMOND, F.; TAYLOR, R. **Fermat’s Last Theorem**. 2007. Disponível em: <<http://www.math.mcgill.ca/darmon/pub/Articles/Expository/05.DDT/paper.pdf>>. Nenhuma citação no texto.
- DAVYDOV, A. **Twisted automorphisms of group algebras**. 2018. Disponível em: <<https://arxiv.org/abs/0708.2758v1>>. Citado na página 106.
- DELAUNAY, C. Heuristics on class groups and on Tate-Shafarevich groups: The magic of the Cohen-Lenstra heuristics. **Exp. Math.**, v. 10, n. 2, p. 191–196, 2001. Citado na página 130.
- DIAMOND, F.; SHURMAN, J. **A First Course in Modular Forms**. 3a. ed. Nova Iorque: Springer, 2005. (Graduate Texts in Mathematics, 228). Citado nas páginas 48, 50, 52, 53, 54, 59, 60, 68 e 82.

- DICKSON, L. E. **History of the Theory of Numbers II: Diophantine analysis**. Nova Iorque: Chelsea Publishing Company, 1971. Citado na página 163.
- DIKRANJAN, D. **Introduction to Topological Groups**. 2009. Disponível em: <<https://users.dimi.uniud.it/~dikran.dikranjan/ITG.pdf>>. Citado na página 30.
- DOKCHITSER, T. **Notes on the Parity Conjecture**. 2012. Disponível em: <<https://arxiv.org/abs/1009.5389>>. Citado na página 120.
- DOKCHITSER, T.; DOKCHITSER, V. On the Birch–Swinnerton-Dyer quotients modulo squares. **Ann. of Math.**, v. 172, n. 1, p. 567–596, 2010. Citado na página 121.
- DUJELLA, A. **History of elliptic curves rank records**. 2009. Disponível em: <<https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html>>. Citado na página 78.
- DUMMIT, D. S.; FOOTE, R. M. **Abstract Algebra**. 3a. ed. Hoboken: John Wiley & Sons, 2004. Citado na página 112.
- ELKIES, N. **Three lectures on elliptic surfaces and curves of high rank**. 2007. Disponível em: <<https://arxiv.org/abs/0709.2908>>. Nenhuma citação no texto.
- ENDLER, O. **Valuation Theory**. Berlim: Springer, 1972. Nenhuma citação no texto.
- ENGLER, A. J.; PRESTEL, A. **Valued Fields**. Berlim: Springer, 2005. (Springer Monographs in Mathematics). Citado na página 35.
- FALTINGS, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. **Inv. Math.**, v. 73, n. 3, p. 349–366, 1983. Citado na página 77.
- FONTAINE, J.-M.; OUYANG, Y. **Theory of p -adic Galois Representations**. 2007. Disponível em: <<https://www.math.u-psud.fr/~fontaine/galoisrep.pdf>>. Nenhuma citação no texto.
- FUCHS, L. **Infinite Abelian Groups**. Nova Iorque: Academic Press, 1970. v. 1. Citado na página 35.
- FULTON, W. **Algebraic Curves: an Introduction to Algebraic Geometry**. 2008. Disponível em: <<http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf>>. Citado nas páginas 23 e 159.
- FULTON, W.; HARRIS, J. **Representation Theory: A first course**. Nova Iorque: Springer, 1991. Citado na página 51.
- GOUVÊA, F. Q. **p -adic Numbers: an Introduction**. 2a. ed. Berlim: Springer, 1997. Citado nas páginas 39, 40, 41, 42, 45 e 46.
- GREENBERG, R. **Topics in Iwasawa Theory**. 2010. Disponível em: <<https://sites.math.washington.edu/~greenber/book.pdf>>. Citado na página 111.
- GREENBERG, R.; STEVENS, G. p -adic L-functions and p -adic periods of modular forms. **Inv. Math.**, v. 111, p. 407–447, 1993. Citado na página 76.
- GRIGOROV, G.; JORZA, A.; PATRIKIS, S.; STEIN, W. A.; TARNITA-PATRASCU, C. **Computational Verification of The Birch and Swinnerton-Dyer Conjecture for Individual Elliptic Curves**. 2009. Disponível em: <<https://wstein.org/papers/bsdalg/bsdalg2.pdf>>. Citado nas páginas 161 e 162.

- GROSS, B.; ZAGIER, D. Heegner points and derivatives of L-series. **Inv. Math.**, v. 84, n. 2, p. 225–320, 1986. Citado nas páginas 20 e 85.
- HALMOS, P. R. **Measure Theory**. Nova Iorque: Springer, 1950. (Graduate Texts in Mathematics, 18). Citado na página 118.
- HATCHER, A. **Algebraic Topology**. 2001. Disponível em: <<https://www.math.cornell.edu/~hatcher/AT/AT.pdf>>. Citado na página 34.
- HEATH-BROWN, D. R. **The Average Analytic Rank of Elliptic Curves**. 2003. Disponível em: <<https://arxiv.org/abs/math/0305114>>. Citado na página 122.
- HEWITT, E.; ROSS, K. A. **Abstract Harmonic Analysis I**. 2a. ed. Nova Iorque: Springer, 1979. v. 15. (Grundlehren der mathematischen Wissenschaften, v. 15). Citado na página 109.
- HSU, J.; MILLER, S. **Ranks of Elliptic Curves and the Birch and Swinnerton-Dyer conjecture**. 2003. Disponível em: <http://web.math.princeton.edu/mathlab/jr01/arank/arank_jon.pdf>. Citado na página 83.
- HUSEMÖLLER, D. **Elliptic Curves**. 2a. ed. Nova Iorque: Springer, 2004. (Graduate Texts in Mathematics, 111). Citado nas páginas 62 e 90.
- IRELAND, K.; ROSEN, M. **A Classic Introduction to Modern Number Theory**. 2a. ed. Nova Iorque: Springer, 1990. (Graduate Texts in Mathematics, 84). Nenhuma citação no texto.
- KATO, K. p-adic Hodge theory and values of zeta functions of modular forms. **Astérisque**, n. 295, p. 117–290, 2004. Citado na página 114.
- KLAGSBRUN, Z.; SHERMAN, T.; WEIGANDT, J. **The Elkies curve has rank 28 subject only to GHR**. 2016. Disponível em: <<https://arxiv.org/abs/1606.07178>>. Citado na página 79.
- KOBLITZ, N. **Introduction to Elliptic Curves and Modular Forms**. 2a. ed. Nova Iorque: Springer, 1993. (Graduate Texts in Mathematics, 97). Citado na página 164.
- KOLYVAGIN, V. Finiteness of $E(\mathbb{Q})$ and $\text{III}(E)$ for a subclass of Weil curves. **Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya**, v. 52, n. 3, p. 522–540, 1988. Citado nas páginas 20 e 105.
- KUBERT, D. S. Universal bounds on the torsion of elliptic curves. **Compos. Math.**, v. 38, n. 1, p. 121–128, 1979. Citado na página 78.
- LANG, S. **Fundamentals of Diophantine Geometry**. Nova Iorque: Springer, 1983. Citado na página 128.
- _____. **Algebraic Number Theory**. 2a. ed. Nova Iorque: Springer, 1986. (Graduate Texts in Mathematics, 110). Citado na página 54.
- _____. **Algebra**. 3a. ed. Nova Iorque: Springer, 2002. (Graduate Texts in Mathematics, 211). Citado nas páginas 30, 34, 99 e 109.
- LEHMER, D. H. Ramanujan's function $\tau(n)$. **Duke Math. J.**, v. 10, n. 3, p. 483–492, 1943. Citado na página 49.
- LORENZINI, D. Torsion and Tamagawa Numbers. **Ann. Inst. Fourier**, v. 61, n. 5, p. 1995–2037, 2011. Citado na página 160.

- MANIN, Y. I.; PANCHISHKIN, A. A. **Introduction to Modern Number Theory**: Fundamental problems, ideas and theories. 2a. ed. Berlim: Springer, 2007. (Encyclopaedia of Mathematical Sciences, Number Theory I). Nenhuma citação no texto.
- MARTINEZ, F. B.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. **Teoria dos Números**: Um passeio com primos e outros números familiares pelo mundo inteiro. Rio de Janeiro: IMPA, 2013. Citado nas páginas 80 e 87.
- MAZUR, B. Rational isogenies of prime degree. **Inv. Math.**, v. 44, n. 2, p. 129–162, 1978. Citado na página 78.
- _____. On the passage from local to global in number theory. **Bull. Amer. Math. Soc. (N.S.)**, v. 29, n. 1, p. 14–50, 1993. Citado na página 101.
- MAZUR, B.; TATE, J.; TEITELBAUM, J. On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer. **Inv. Math.**, v. 84, p. 1–48, 1986. Citado na página 76.
- MCCARTY, G. **Topology**: An introduction with application to topological groups. Nova Iorque: Dover Publications, 1988. Citado na página 109.
- MILNE, J. S. **Elliptic Curves**. 2006. Disponível em: <<https://www.jmilne.org/math/Books/ectext6.pdf>>. Nenhuma citação no texto.
- _____. **Class Field Theory**. 2013. Disponível em: <<https://www.jmilne.org/math/CourseNotes/CFT.pdf>>. Citado nas páginas 31 e 32.
- _____. **Algebraic Number Theory**. 2017. Disponível em: <<https://www.jmilne.org/math/CourseNotes/ANT.pdf>>. Citado na página 42.
- _____. **Fields and Galois Theory**. 2018. Disponível em: <<https://www.jmilne.org/math/CourseNotes/FT.pdf>>. Citado na página 30.
- MIRANDA, R. **Algebraic Curves and Riemann Surfaces**. Providence, RI: American Mathematical Society, 1995. (Graduate Studies in Mathematics, 5). Citado na página 68.
- MIYAKE, T. **Modular Forms**. 2a. ed. Berlim: Springer, 2006. (Springer Monographs in Mathematics). Citado na página 54.
- MONSKY, P. **Generalizing the Birch-Stephens theorem. I. Modular curves**. 1996. 415–420 p. Citado na página 120.
- MORRIS, S. A. **Pontryagin Duality and the Structure of Locally Compact Abelian Groups**. Cambridge: Cambridge University Press, 1977. v. 29. (London Mathematical Society Lecture Note Series, v. 29). Citado nas páginas 109 e 110.
- NEUKIRCH, J. **Algebraic Number Theory**. Berlim: Springer, 2009. Citado nas páginas 42, 43, 45 e 85.
- PARK, J.; POONEN, B.; VOIGHT, J.; WOOD, M. M. **A heuristic for boundness of ranks of elliptic curves**. 2018. Disponível em: <<https://arxiv.org/abs/1602.01431>>. Citado na página 78.
- POONEN, B. **The Selmer group, the Shafarevich-Tate group, and the Weak Mordell-Weil theorem**. 2002. Disponível em: <<http://math.univ-lyon1.fr/~roblot/ihp/weakmw.pdf>>. Citado na página 105.

_____. **Lectures on rational points on curves**. 2006. Disponível em: <<https://math.mit.edu/~poonen/papers/curves.pdf>>. Citado na página 100.

_____. **Average rank of elliptic curves**. 2015. Disponível em: <<https://arxiv.org/abs/1203.0809>>. Nenhuma citação no texto.

_____. **Heuristics for the Arithmetic of Elliptic Curves**. 2017. Disponível em: <<https://arxiv.org/abs/1711.10112>>. Nenhuma citação no texto.

POONEN, B.; RAINS, E. Random maximal isotropic subspaces and Selmer groups. 2011. Disponível em: <<https://arxiv.org/abs/1009.0287>>. Citado na página 130.

POONEN, B.; STOLL, M. **The Cassels–Tate pairing on polarized abelian varieties**. 1999. 1109–1149 p. Disponível em: <<https://arxiv.org/abs/math/9911267>>. Citado na página 106.

RIBES, L. Introduction to profinite groups. **Trav. Math.**, v. 22, p. 179–230, 2013. Citado na página 31.

RIBET, K.; STEIN, W. **Lectures on Serre’s Conjectures**. 1999. Disponível em: <<https://wstein.org/papers/serre/ribet-stein.pdf>>. Nenhuma citação no texto.

_____. **Lectures on Modular Forms and Hecke Operators**. 2017. Disponível em: <<https://wstein.org/books/ribet-stein/main.pdf>>. Nenhuma citação no texto.

RUBIN, K. The ‘main conjectures’ of Iwasawa theory for imaginary quadratic fields. **Inv. Math.**, v. 102, n. 1, p. 25–68, 1991. Citado nas páginas 20 e 105.

RUBIN, K.; SILVERBERG, A. Ranks of elliptic curves. **Bull. Amer. Math. Soc. (N.S.)**, v. 39, n. 4, p. 455–474, 2002. Nenhuma citação no texto.

SARNAK, P. **Problems of the Millennium: The Riemann Hypothesis**. 2004. Disponível em: <https://www.claymath.org/sites/default/files/sarnak_rh_0.pdf>. Citado na página 53.

SEARCOID, M. . **Metric Spaces**. Londres: Springer, 2007. (Springer Undergraduate Mathematics Series). Citado na página 38.

SERRE, J.-P. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. **Inv. Math.**, v. 15, p. 259–331, 1972. Nenhuma citação no texto.

_____. **A Course in Arithmetic**. Nova Iorque: Springer, 1973. (Graduate Texts in Mathematics, 7). Citado nas páginas 48, 49, 50, 51, 83 e 138.

_____. **Local Fields**. Nova Iorque: Springer, 1979. (Graduate Texts in Mathematics, 67). Nenhuma citação no texto.

_____. **Abelian ℓ -Adic Representations and Elliptic Curves**. Redwood City, CA: Addison-Wesley Publishing Company, 1989. Citado na página 90.

_____. **Galois Cohomology**. Berlim: Springer, 1997. (Springer Monographs in Mathematics). Citado na página 31.

SHAFAREVICH, I. R. **Basic Algebraic Geometry 1: Varieties in projective space**. 3a. ed. Berlim: Springer, 2013. Nenhuma citação no texto.

- SHIMURA, G. **Introduction to the Arithmetic Theory of Automorphic Functions**. Princeton: Addison-Wesley Publishing Company, 1971. (Publications of the Mathematical Society of Japan, 11). Nenhuma citação no texto.
- SILVERBERG, A. **Ranks “cheat sheet”**. 2013. Disponível em: <https://www.math.uci.edu/~asilverb/bibliography/RanksCheatSheet.pdf>. Nenhuma citação no texto.
- SILVERMAN, J. H. **Advanced Topics in the Arithmetic of Elliptic Curves**. Nova Iorque: Springer, 1994. (Graduate Texts in Mathematics, 151). Citado nas páginas 74 e 162.
- _____. **The Arithmetic of Elliptic Curves**. 2a. ed. Nova Iorque: Springer, 2009. (Graduate Texts in Mathematics, 106). Citado nas páginas 31, 33, 62, 63, 65, 67, 81, 93, 102, 104, 105, 125, 157, 159 e 161.
- SILVERMAN, J. H.; TATE, J. T. **Rational Points on Elliptic Curves**. 2a. ed. Cham, Suíça: Springer, 2015. Citado na página 79.
- SKINNER, C. **A converse to a theorem of Gross, Zagier and Kolyvagin**. 2014. Disponível em: <https://arxiv.org/abs/1405.7294v1>. Citado na página 105.
- _____. **Multiplicative reduction and the cyclotomic main conjecture for modular forms**. 2014. Disponível em: <https://arxiv.org/abs/1407.1093>. Citado na página 114.
- _____. **Lectures on the Iwasawa theory of elliptic curves**. 2018. Disponível em: <http://swc.math.arizona.edu/aws/2018/2018SkinnerNotes.pdf>. Nenhuma citação no texto.
- SKINNER, C.; URBAN, E. **The Iwasawa main conjectures for GL_2** . 2014. 1-277 p. Disponível em: <http://www.math.columbia.edu/~urban/eurp/MC.pdf>. Citado na página 114.
- SKINNER, C.; ZHANG, W. **Indivisibility of Heegner points in the multiplicative case**. 2014. Disponível em: <https://arxiv.org/abs/1407.1099>. Citado na página 125.
- SNOWDEN, A. **Course on Mazur’s theorem**. 2013. Disponível em: <http://www-personal.umich.edu/~asnowden/teaching/2013/679/>. Citado na página 78.
- Stacks project authors, T. **The Stacks project**. 2020. Disponível em: <https://stacks.math.columbia.edu>. Citado na página 108.
- STEIN, W. **Algebraic Number Theory, a Computational Approach**. 2010. Disponível em: https://wstein.org/edu/2010/581b/stein-algebraic_number_theory.pdf. Citado na página 43.
- _____. **The Birch and Swinnerton-Dyer Conjecture, a Computational Approach**. 2016. Disponível em: <https://williamstein.org/books/bsd/bsd.pdf>. Citado na página 88.
- STEIN, W.; WUTHRICH, C. **Heuristics for the Arithmetic of Elliptic Curves**. 2013. Disponível em: <https://wstein.org/papers/shark/shark.pdf>. Citado na página 107.
- TATE, J. Algorithm for determining the type of a singular fiber in an elliptic pencil. In: BIRCH, B.; KUYK, W. (Ed.). **Modular Functions of One Variable IV: Proceedings of the International Summer School, University of Antwerp, RUCA, July 17 - August 3, 1972**. Berlim: Springer, 1975. p. 33–52. Citado na página 157.
- TAYLOR, R.; WILES, A. Ring-theoretic properties of certain Hecke algebras. **Ann. of Math.**, v. 141, n. 3, p. 553–572, 1995. Citado nas páginas 19 e 82.

TENGAN, E. **An Invitation to Local Fields**. 2008. Disponível em: <http://www.mtm.ufsc.br/xja/arquivos/tengan_prerequisitos.pdf>. Citado na página 100.

The LMFDB Collaboration. **The L -functions and Modular Forms Database**. 2013. Disponível em: <<http://www.lmfdb.org>>. Nenhuma citação no texto.

The PARI Group. **PARI/GP version 2.11.0**. Universidade de Bordeaux: [s.n.], 2018. Disponível em: <<http://pari.math.u-bordeaux.fr/>>. Nenhuma citação no texto.

_____. **User's Guide to PARI/GP (version 2.11.0)**. 2018. Disponível em: <<https://pari.math.u-bordeaux.fr/pub/pari/manuals/2.11.1/users.pdf>>. Citado na página 76.

TUNNELL, J. B. A classical diophantine problem and modular forms of weight $3/2$. **Inv. Math.**, v. 72, n. 2, p. 323–334, 1983. Citado na página 163.

VILLEGAS, F. R.; ZAGIER, D. **Which primes are sums of two cubes?** 1995. Disponível em: <<https://people.mpim-bonn.mpg.de/zagier/files/mpim/95-61/fulltext.pdf>>. Citado na página 165.

WAN, X. **Introduction to Skinner-Urban's Work on the Iwasawa Main Conjecture for GL_2** . 2016. Disponível em: <<http://www.mcm.ac.cn/faculty/wx/201609/W020160919378831326945.pdf>>. Citado na página 114.

WASHINGTON, L. C. **Elliptic Curves, Number Theory and Cryptography**. 2a. ed. [S.l.]: CRC Press, 2008. Citado nas páginas 63, 69, 70, 84, 86, 128, 158 e 160.

WIESE, G. **Galois Representations**. 2012. Disponível em: <<http://math.uni.lu/~wiese/notes/GalRep.pdf>>. Citado na página 44.

WILES, A. Modular elliptic curves and Fermat's Last Theorem. **Ann. of Math.**, v. 141, n. 3, p. 443–551, 1995. Citado na página 82.

_____. **The Birch and Swinnerton-Dyer Conjecture**. 2000. Disponível em: <<https://www.claymath.org/sites/default/files/birchswin.pdf>>. Citado na página 19.

YOUNG, M. P. **Low-lying zeros of families of elliptic curves**. 2004. Disponível em: <<https://arxiv.org/abs/math/0406330>>. Citado na página 122.

ZHANG, W. **Selmer groups and the indivisibility of Heegner points**. 2014. 191–253 p. Disponível em: <<http://math.mit.edu/~wz2113/math/online/Kconj.pdf>>. Citado na página 125.

MAIS SOBRE A CONJECTURA BSD

A.1 A conjectura forte de Birch e Swinnerton-Dyer

Nesta seção, E é curva elíptica sobre $\mathbb{Q}$. A conjectura forte de Birch e Swinnerton-Dyer é um refinamento da conjectura [BSD](#) que, além de postular que $r_{\text{alg}}(E)$ é a ordem de $L(s, E)$ em $s = 1$, determina o coeficiente líder de $L(s, E)$ (portanto, o $r_{\text{alg}}(E)$ -ésimo coeficiente) em termos de diversas quantidades associadas a E , que serão definidas abaixo.

A.1.1 Regulador elíptico

Recorde a altura canônica de Néron–Tate:

$$\widehat{h}(P) = \lim_{n \rightarrow \infty} \frac{h_x(2^n P)}{4^n},$$

onde h_x é a altura logarítmica de E (Definição [3.1.8](#)).

Proposição A.1.1. A altura canônica de Néron–Tate satisfaz a Lei do Paralelogramo, isto é,

$$\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q),$$

com $P, Q \in E(\overline{\mathbb{Q}})$.

Prova. Pela definição de altura,

$$h_x(P+Q) + h_x(P-Q) \leq (2h_x(Q) + C_1(P)) + (2h_x(P) + C_1(-Q)) = 2h_x(P) + 2h_x(Q) + C(P, Q),$$

onde $C(P, Q)$ é uma constante. Logo, para quaisquer $P, Q \in E(\mathbb{Q})$,

$$\begin{aligned} \frac{h_x(2^n P + 2^n Q) + h_x(2^n P - 2^n Q)}{4^n} &\leq \frac{2h_x(2^n P) + 2h_x(2^n Q) + C(P, Q)}{4^n} \\ &\xrightarrow{n \rightarrow \infty} \widehat{h}(P+Q) + \widehat{h}(P-Q) \leq 2\widehat{h}(P) + 2\widehat{h}(Q). \end{aligned}$$

Usando esta desigualdade para $P' = P+Q$ e $Q' = P-Q$ nos dá a desigualdade inversa e, portanto, a igualdade. ■

Corolário A.1.2. O pareamento $\langle \cdot, \cdot \rangle : E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \rightarrow \mathbb{R}$ dado por

$$\langle P, Q \rangle = \frac{1}{2}(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q))$$

é bilinear e não-degenerado. É chamado **pareamento de Néron–Tate**.

Prova. Note que $\widehat{h}$ é par (coloque $P = O$ na Lei do Paralelogramo). Para a bilinearidade, basta mostrar que $\langle P+R, Q \rangle = \langle P, Q \rangle + \langle R, Q \rangle$, pois o pareamento é claramente simétrico. Para isto, usamos estrategicamente a Lei do Paralelogramo para obter as seguintes equações:

$$\begin{aligned} \widehat{h}((P+R)+Q) + \widehat{h}((P+R)-Q) &= 2\widehat{h}(P+R) + 2\widehat{h}(Q) \\ \widehat{h}(P+(Q-R)) + \widehat{h}(P-(Q-R)) &= 2\widehat{h}(P) + 2\widehat{h}(Q-R) \\ \widehat{h}((P+Q)+R) + \widehat{h}((P+Q)-R) &= 2\widehat{h}(P+Q) + 2\widehat{h}(R) \\ 2\widehat{h}(R+Q) + 2\widehat{h}(R-Q) &= 4\widehat{h}(R) + 4\widehat{h}(Q) \end{aligned}$$

que, somadas alternadamente, nos dão

$$\widehat{h}(P+Q+R) - \widehat{h}(P+Q) - \widehat{h}(P+R) - \widehat{h}(R+Q) + \widehat{h}(P) + \widehat{h}(Q) + \widehat{h}(R) = 0,$$

o que implica o resultado buscado. ■

Considere o quociente $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tor}}$ (isto é, apenas a parte livre de $E(\mathbb{Q})$) e sejam $\{P_1, \dots, P_r\}$ um conjunto de (finitos) geradores (Teorema de Mordell–Weil, 3.1.1).

Definição A.1.3. Se $r > 0$, o **regulador elíptico** de E é definido pelo Determinante de Gram

$$\text{Reg}(E) \doteq \left| \det \begin{bmatrix} \langle P_1, P_1 \rangle & \cdots & \langle P_1, P_j \rangle & \cdots & \langle P_1, P_r \rangle \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \langle P_i, P_1 \rangle & \cdots & \langle P_i, P_j \rangle & \cdots & \langle P_i, P_r \rangle \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \langle P_r, P_1 \rangle & \cdots & \langle P_r, P_j \rangle & \cdots & \langle P_r, P_r \rangle \end{bmatrix} \right|.$$

Se $r = 0$, convencionamos $\text{Reg}(E) \doteq 1$.

O regulador elíptico pode ser interpretado como o volume de um domínio fundamental para o quociente $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tor}}$, que é um reticulado^[226] no $\mathbb{R}$ -espaço vetorial $E(\mathbb{Q}) \otimes \mathbb{R}$, que tem dimensão $r_{\text{alg}}(E) < \infty$. Como os geradores são independentes e $\langle \cdot, \cdot \rangle$ é não-degenerado em $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tor}}$ (pois $\widehat{h}(P) = 0 \iff P$ é de torção), $\text{Reg}(E) > 0$.

^[226]Um **reticulado** num $\mathbb{R}$ -espaço vetorial V de dimensão finita é o $\mathbb{Z}$ -módulo gerado por uma base de V .

A.1.2 Números de Tamagawa

Seja p primo, tome um modelo minimal global para E e veja E como uma curva elíptica sobre $\mathbb{Q}_p$. Denote por $E_0(\mathbb{Q}_p)$ o subgrupo de $E(\mathbb{Q}_p)$ formados pelos pontos que têm redução módulo p não-singular.

Teorema A.1.4 (Kodaira–Néron^[227]). O quociente $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ é finito.

Definição A.1.5. Definimos o **número de Tamagawa** $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$.^[228]

Na prática, os números de Tamagawa são calculados por um algoritmo devido a Tate (TATE, 1975). O comando `elllocalred(E,p)` do PARI/GP retorna, entre outras coisas, c_p como a última entrada do *output*.

A.1.3 Período real

A.1.3.1 Componentes conexas de uma curva elíptica sobre $\mathbb{R}$

Uma curva elíptica E sobre $\mathbb{R}$ pode ser vista como uma curva elíptica sobre $\mathbb{C}$ e, portanto, como um toro complexo $\mathbb{C}/\Lambda_\tau$, para algum $\tau \in \mathbb{H}$ (ver seção 2.3).

Um domínio fundamental (ver nota [66]) para a ação de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathbb{H}$ é dado por

$$\mathcal{D} = \left\{ z \in \mathbb{H}; -\frac{1}{2} \leq \mathrm{Re}(z) \leq 0, |z| \geq 1 \right\} \cup \left\{ z \in \mathbb{H}; 0 < \mathrm{Re}(z) < \frac{1}{2}, |z| > 1 \right\}.$$

Figura 5 – Domínio fundamental usual para a ação de $\mathrm{SL}_2(\mathbb{Z})$ sobre $\mathbb{H}$

Fonte: Elaborada pelo autor.

^[227]O Teorema de Kodaira–Néron, além de dizer que $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ é finito, também especifica que a ordem deste grupo é $v_p(\Delta(E))$ se E tem redução multiplicativa *split* em p , e ≤ 4 caso contrário (SILVERMAN, 2009, p. 200, Teorema VII.6.1).

^[228]Birch e Swinnerton-Dyer originalmente chamavam estes números de “fatores de correção” (*fudge factors*). Note que $c_p = 1$ para todos exceto finitos primos (pois E tem redução má apenas em finitos primos). Mesmo assim, é possível que $c_p = 1$ para um primo p onde E tenha redução má (Veja Exemplo A.1.11 a seguir).

Vamos supor $\tau \in \mathcal{D}$. O fato de E estar definida sobre $\mathbb{R}$ impõe condições a τ :

Proposição A.1.6. $E \stackrel{\mathbb{C}}{\cong} E_\tau$ está definida sobre $\mathbb{R} \iff \operatorname{Re}(\tau) \in \left\{0, \frac{1}{2}\right\}$.

Prova. [229] Como E está definida sobre $\mathbb{R}$, $j(E) = j(E_\tau) = j(\tau) \in \mathbb{R}$. Note que $\overline{j(z)} = j(-\bar{z})$, isto é, “reflexão em torno do eixo vertical conjuga o j ”. Logo, se τ está no interior de $\mathcal{D}$, então $\operatorname{Re}(\tau) = 0$. Se τ estiver na parte inferior da borda (isto é, $\tau \in \{z \in \mathbb{H}; |z| = 1, -\frac{1}{2} \leq \operatorname{Re}(z) < 0\}$), podemos trocá-lo pelo $\operatorname{SL}_2(\mathbb{Z})$ -equivalente

$$\tau' = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tau, \text{ que satisfaz } \operatorname{Re}(\tau') = \frac{1}{2}.$$

Para a recíproca, note que, se $\operatorname{Re}(\tau) \in \left\{0, \frac{1}{2}\right\}$, $q = e^{2\pi i \tau} \in \mathbb{R}$. Como os coeficientes da expansão de Fourier de g_2 e g_3 são reais (Exemplo 1.7.5), segue que $g_2(\tau), g_3(\tau) \in \mathbb{R}$. ■

Figura 6 – Possibilidades para τ se E_τ está definida sobre $\mathbb{R}$.

Fonte: Elaborada pelo autor.

Figura 7 – Pontos a que o traço real de E corresponde no toro $\mathbb{C}/\Lambda_\tau$.

Fonte: Elaborada pelo autor.

[229] Seguindo o roteiro apresentado em Washington (2008), p. 308, Exercício 9.5.

Grosso modo, no primeiro caso, $\mathbb{P}^2(\mathbb{R})$ corta o toro (visto em $\mathbb{P}^2(\mathbb{C})$) passando pelo furo no centro, resultando em duas componentes conexas, enquanto que no segundo caso, $\mathbb{P}^2(\mathbb{R})$ não passa pelo furo, resultando em apenas uma componente conexa:

Figura 8 – As possíveis formas de uma curva elíptica real.

Fonte: Elaborada pelo autor.

Conforme o Exemplo 2.1.2, $E_1: y^2 = x^3 - x$ é uma curva elíptica do primeiro tipo e $E_2: y^2 = x^3 - 3x + 3$ é uma curva elíptica do segundo. Observe que

$$\Delta(E_1) = 64 > 0 \quad \text{e} \quad \Delta(E_2) = -2160 < 0.$$

De fato, o discriminante nos dá um critério simples para saber quantas componentes conexas uma curva elíptica sobre $\mathbb{R}$ possui:

Proposição A.1.7. Seja E uma curva elíptica. Temos os isomorfismos

$$E(\mathbb{R}) \cong \begin{cases} \mathbb{R}/\mathbb{Z}, & \text{se } \Delta(E) < 0 \\ (\mathbb{R}/\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), & \text{se } \Delta(E) > 0 \end{cases}$$

(SILVERMAN, 2009, p. 420, Corolário V.2.3.1).

No segundo caso, o fator $\mathbb{Z}/2\mathbb{Z}$ indica em qual componente conexa se está.

A.1.3.2 Definição do período real

Suponha que E está num modelo minimal global.

Definição A.1.8. Seja γ a componente conexa de O em $E(\mathbb{R})$. O **período real** de E é $\omega_E \doteq \int_{\gamma} \eta$, onde $\eta \doteq \frac{dx}{2y + a_1x + a_3}$.^[230]

^[230]Para mais detalhes sobre esta diferencial, veja Silverman (2009), Capítulo III e, para diferenciais sobre variedades algébricas em geral, veja Fulton (2008), Seção 8.4.

Mas este não é exatamente o número que estamos procurando: queremos integrar a diferencial η sobre todos os pontos da curva $E(\mathbb{R})$. Definimos a variante^[231]

$$\Omega_E \doteq \int_{E(\mathbb{R})} |\eta|,$$

que vale ω_E vezes o número de componentes conexas de $E(\mathbb{R})$, que descrevemos acima.

Na prática, existe um algoritmo baseado na média aritmético-geométrica para se calcular Ω_E : dados $a, b \in \mathbb{R}_{>0}$, defina

$$a_0 = a, \quad b_0 = b, \quad a_n = \frac{1}{2}(a_{n-1} + b_{n-1}) \quad \text{e} \quad b_n = \sqrt{a_{n-1}b_{n-1}}.$$

A **média aritmético-geométrica** de a e b é dada por

$$M(a, b) = \lim_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} b_n.$$

Se $E: y^2 = 4(x - e_1)(x - e_2)(x - e_3)$ tem três raízes reais ($\Delta(E) > 0$),

$$\omega_1 = \frac{\pi}{M(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})} \quad \text{e} \quad \omega_2 = i\omega_1$$

geram um reticulado para E . Se $\Delta(E) < 0$ e e_1 é a única raiz real,

$$\omega_1 = \frac{2\pi}{M(2\sqrt{b}, \sqrt{b+2a})} \quad \text{e} \quad \omega_2 = -\frac{\omega_1}{2} + \frac{\pi i}{M(2\sqrt{b}, \sqrt{b-2a})},$$

onde $a = 3e_1 + \frac{b_2}{4}$ e $b = \sqrt{3e_1^2 + \frac{b_2}{2}e_1 + \frac{b_4}{2}}$, geram um reticulado para E . Em ambos os casos, $\omega_1 = \omega_E$, o que justifica seu nome (COHEN, 1996, p. 398, Algoritmo 7.4.7), (WASHINGTON, 2008, p. 286, Seção 9.4).

Observação A.1.9. O “fator de correção” pelo qual multiplicamos o período real de E pode ser interpretado como sendo o Número de Tamagawa no lugar ∞ : definido-se

$$c_\infty = \begin{cases} 1, & \text{se } \Delta(E) > 0 \\ 2, & \text{se } \Delta(E) < 0 \end{cases},$$

temos que $\Omega_E = c_\infty \omega_E$ (LORENZINI, 2011, p. 2001, Remark 2.6).

A.1.4 A conjectura

Agora, estamos prontos para enunciar a conjectura BSD forte:

Conjectura A.1.10 (Birch e Swinnerton-Dyer, forte). Seja E uma curva elíptica sobre $\mathbb{Q}$. Então, $r_{\text{alg}}(E) = r_{\text{an}}(E) \doteq r$ e, com a notação anterior,

$$\lim_{s \rightarrow 1} \frac{L(s, E)}{(s-1)^r} = \frac{\Omega_E \cdot \#\text{III}(E) \cdot \text{Reg}(E) \cdot \prod_{p \text{ primo}} c_p}{\#E(\mathbb{Q})_{\text{tor}}^2}.$$

^[231]O número Ω_E não tem um nome específico. Só para termos do que chamá-lo, diremos que Ω_E é o **período real corrigido de E** .

Em 1974, Tate afirmou que “esta notável conjectura relaciona o comportamento de uma função L num ponto em que atualmente não se sabe se está definida à ordem de um grupo III que não se sabe ser finito!”. Desde então, muito mudou: já sabemos, graças ao Teorema da Modularidade (Teorema 3.2.3), que $L(s, E)$ está definida em $s = 1$, mas, como vimos, a finitude da ordem do grupo de Tate–Shafarevich ainda está em aberto no caso geral (Conjectura 4.3.16).

A conjectura BSD forte já foi checada computacionalmente para diversos casos particulares^[232]. A título de exemplo, vamos checá-la para um exemplo concreto, usando o PARI/GP para fazer os cálculos.^[233]

Exemplo A.1.11. Considere a curva elíptica $E: y^2 = x^3 - 4x + 4$ (LMFDB 88.a1), que está num modelo minimal global.

- Começamos calculando o discriminante, que é $\Delta = -2816 = -2^8 \cdot 11$;
- Vamos investigar a torção. Pelo Teorema de Nagell–Lutz (Teorema 3.3.1), se $(x_0, y_0) \in E(\mathbb{Q})$ é de torção, então $x_0, y_0 \in \mathbb{Z}$ e $y_0 = 0$ ou $y_0 \mid \Delta$. Usando técnicas de Cálculo (ou uma calculadora que compute raízes de polinômios!), vemos que os únicos valores de y_0 dentre estes que nos dão pontos na curva são ± 2 , para os quais temos $x_0 \in \{-2, 0, 2\}$. Usando o PARI/GP, observamos que nenhum destes pontos é de torção (em algum momento, somando-os consigo mesmos^[234], obtemos pontos cujas coordenadas não são inteiras). Logo, $\#E(\mathbb{Q})_{\text{tor}} = 1$. Além disso, notamos que $(2, -2) = -(2, 2)$ e que $[2](2, \pm 2) = (0, \pm 2)$, o que nos faz suspeitar de que $(2, -2)$ gera a parte livre, isto é, $r_{\text{alg}}(E) = 1$;
- Usando o comando `ellanalyticrank(E)`, obtemos que $r_{\text{an}}(E) = 1$ e que $L'(E, 1) \approx 0,6849015939041220693022740667$. Em particular, pelo Teorema de Kolyvagin–Rubin (Teorema 4.3.17), a conjectura BSD fraca vale para E , donde $r_{\text{alg}}(E) = 1$, e $\#\text{III}(E) < \infty$;
- Usando a fórmula de duplicação^[235] para determinar se existe $P \in E(\mathbb{Q})$ tal que $x([2]P) = 2$, obtemos uma equação quártica sem raízes em $\mathbb{Q}$. Logo, $(2, -2)$ não é o dobro de nenhum ponto. Portanto, gera $E(\mathbb{Q})/2E(\mathbb{Q})$. Pela Proposição 3.3.4, $(2, -2)$ gera $E(\mathbb{Q})$;
- Usando o comando `ellheight(E, [x0,y0])`, obtemos que

$$\hat{h}(2, -2) \approx 0.04026436433688064294321515224$$

^[232]Por exemplo, Grigorov *et al.* (2009) mostraram que a conjectura vale para todas as curvas elípticas E sobre $\mathbb{Q}$ sem multiplicação complexa, com $r_{\text{alg}}(E) \leq 1$ e $N_E \leq 1000$ e que satisfazem algumas condições locais (Teorema A.1.12 adiante).

^[233]No LMFDB estão disponíveis para cada curva elíptica indexada todos os parâmetros relacionados à fórmula de Birch e Swinnerton-Dyer (exceto, é claro, a ordem do grupo de Tate–Shafarevich, mas apresenta-se seu valor esperado dado pela fórmula).

^[234]Código:

```
E = ellinit([0,0,0,-4,4]);
elladd(E, [x1,y1], [x2,y2])
```

^[235]Esta fórmula expressa a abscissa de $2P$ como uma função racional em termos da abscissa de P e coeficientes dados em termos dos parâmetros b_2, b_4, b_6 e b_8 da curva. Veja, por exemplo, Silverman (2009), p. 54.

Logo, $\text{Reg}(E) = \widehat{h}(2, -2) \approx 0.04026436433688064294321515224$;

- Vamos estudar as reduções de E módulo primos. Analisando o discriminante de E , temos apenas que checar as reduções em 2 e 11, pois as outras são boas. Note que $c_4 = 192$. Logo, a redução em 2 é aditiva e a redução em 11 é multiplicativa;
- Calculemos os números de Tamagawa para estes primos de redução má. Em 11, o gerador de $E(\mathbb{Q})$ se reduz a um ponto não-singular, donde todo ponto deste grupo tem redução não-singular. Logo, $c_{11} = 1$. Em 2, $(2, -2)$ tem redução singular. Pelo Teorema de Kodaira–Néron (Teorema A.1.4), $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ é finito. Procurando o primeiro N tal que $[N](2, -2)$ possui redução não-singular, obtemos $N = 4$. Logo, $c_2 = 4$;
- Usando o comando `E.omega[1]`, obtemos que $\omega_E \approx 4.252529533148360025344953146$. Como $\Delta(E) < 0$, $\omega_E = \Omega_E$;
- Até aqui, a ordem prevista para $\text{III}(E)$ é 1^[236], isto é, $\text{III}(E)$ é trivial. Como, na prática, é difícil calcular este grupo, vamos tentar utilizar o seguinte teorema:

Teorema A.1.12 (Grigorov–Jorza–Patrikis–Stein–Tarniță–Pătrașcu). Seja E uma curva elíptica sobre $\mathbb{Q}$ sem multiplicação complexa (ver nota [127]), com $r_{\text{alg}}(E) \leq 1$ e $N_E \leq 1000$. Para cada p primo ímpar, suponha que $\overline{\rho}_{E,p}$ é irredutível e que $p \nmid c_\ell$ para todo ℓ primo. Então, a ordem prevista para $\text{III}(E)$ pela conjectura BSD forte está correta (GRIGOROV *et al.*, 2009, p. 3, Teorema 1.8).

Agora, vamos checar as hipóteses do teorema para E :

- Usando o comando `ellglobalred(E)`, obtemos que $N_E = 2^3 \cdot 11 = 88 \leq 1000$;
- Como $E(\mathbb{Q})_{\text{tor}} = 0$, $\overline{\rho}_{E,p}$ é irredutível para todo p (Proposição 3.4.6). Além disso, como o único número de Tamagawa não-trivial é $c_2 = 4$, nenhum primo ímpar divide qualquer número de Tamagawa de E ;
- O j -invariante de uma curva elíptica com multiplicação complexa é um inteiro algébrico (SILVERMAN, 1994, p. 40, Teorema II.6.1). Mas $j(E) = -\frac{27648}{11} \notin \mathbb{Z}$, donde E não tem multiplicação complexa;
- Logo, pelo Teorema A.1.12, $\#\text{III}(E) = 1$ e a conjectura BSD forte vale para E !

Veja Cremona (2011) para mais exemplos concretos e outras observações sobre a verificação computacional da Conjectura Forte de Birch e Swinnerton-Dyer^[237].

^[236]Usando os valores acima, obtemos 1 com 28 casas decimais de precisão!

^[237]Nesta palestra, Cremona apresenta um exemplo de curva elíptica para cada posto entre 0 e 4, para mostrar a diferença entre a relativa facilidade entre verificar a conjectura BSD forte para curvas elípticas de posto baixo (0 e 1) para os postos mais altos, onde progressivamente mais e mais ferramentas deixam de funcionar. Veja também (BUHLER; GROSS; ZAGIER, 1985) para a verificação da conjectura BSD forte para uma curva elíptica de posto 3.

A.2 Outras aplicações da conjectura BSD

Diversos problemas dependem da nossa capacidade de calcular o posto algébrico de certas curvas elípticas. Logo, a conjectura BSD, ao nos fornecer uma maneira garantida de calcular posto algébrico, nos dá também a solução de tais problemas. Abaixo, trazemos dois exemplos desta aplicação indireta da conjectura BSD.

A.2.1 Problema do número congruente

O problema do número congruente é um dos mais antigos problemas em aberto na Teoria dos Números: a primeira menção registrada a este problema remonta a um manuscrito árabe de c. 972. Ao longo da História, o problema atraiu a atenção de diversos matemáticos renomados, como Leonardo Fibonacci, Pierre de Fermat, Leonhard Euler e François Lucas ([DICKSON, 1971](#), p. 459).

Definição A.2.1. Um número $n \in \mathbb{Z}_{>0}$ é **congruente** se existe um triângulo retângulo de lados racionais e área n .^[238]

O problema é: *determinar quais são os números congruentes.*

Alguns casos particulares são conhecidos: por exemplo, $n = 1$ foi mostrado não ser congruente por Fermat, usando a técnica da descida infinita ([CONRAD, 2019a](#), p. 3, Teorema 2.1). Existe também um teorema que, na forma contrapositiva, nos dá um critério para dizer quando um número não é congruente ([TUNNELL, 1983](#)):

Teorema A.2.2 (Tunnell). Seja n livre de quadrados^[239] e defina

$$\begin{aligned} A_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 32z^2\}, \\ B_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 8z^2\}, \\ C_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid n = 8x^2 + 2y^2 + 64z^2\}, \\ D_n &= \#\{(x, y, z) \in \mathbb{Z}^3 \mid n = 8x^2 + 2y^2 + 16z^2\}. \end{aligned}$$

Se n é congruente e ímpar, $2A_n = B_n$. Se n é congruente e par, $2C_n = D_n$.

Por exemplo, o teorema acima nos dá que $n = 2019$ não é congruente ($A_{2019} = 88$ e $B_{2019} = 192$). Porém, dizer quando um número é congruente pode não ser tão simples:

^[238]A definição original do problema, que é equivalente a esta apresentada, é: um número n é congruente se existe um quadrado racional q^2 tal que $n \pm q^2$ também são quadrados racionais.

^[239]Note que, dividindo e multiplicando os lados de um triângulo retângulo por p primo, n é congruente se, e somente se, np^2 o é. Em particular, como 1 não é congruente, nenhum quadrado perfeito o é. Daqui em diante, assumiremos que n é sempre livre de quadrados.

Exemplo A.2.3 (Zagier). 157 é congruente. De fato, é a área do triângulo retângulo com lados^[240]

$$\frac{411340519227716149383203}{21666555693714761309610}, \frac{6803298487826435051217540}{411340519227716149383203}, e$$

$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

A Conjectura BSD nos dá a recíproca do Teorema A.2.2. Para isso, precisamos colocar a propriedade de um número ser congruente no contexto das curvas elípticas.

Considere, para cada $n \in \mathbb{Z}_{>0}$, a curva elíptica $E_n: y^2 = x^3 - n^2x$. Por um lado, se n é um número congruente, existe um triângulo retângulo (a, b, c) de área n . Então,

$$P_{(a,b,c)} \doteq \left(\frac{nb}{c-a}, \frac{2n^2}{c-a} \right) \in E_n$$

é um ponto de E_n com coordenadas racionais não-inteiras. Logo, pelo Teorema de Nagell–Lutz (Teorema 3.3.1), $P_{(a,b,c)}$ tem ordem infinita. Logo, $r_{\text{alg}}(E_n) > 0$.

Por outro lado, se $r_{\text{alg}}(E_n) > 0$, podemos tomar um ponto $P = (x, y)$ de ordem infinita e coordenadas positivas. O triângulo retângulo de lados racionais

$$\left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right)$$

tem área n , donde n é congruente. Em suma,

Teorema A.2.4. Um número $n \in \mathbb{Z}_{>0}$ é congruente se, e somente se, $r_{\text{alg}}(E_n) > 0$.

Sabendo calcular $r_{\text{alg}}(E_n)$, que, pela conjectura BSD, é equivalente a saber calcular $L(1, E_n)$, sabemos dizer se um número é congruente ou não.

O *root number* de $L(1, E_n)$ é -1 se $n \equiv 5, 6, 7 \pmod{8}$, e 1 se $n \equiv 1, 2, 3 \pmod{8}$ (KOBLITZ, 1993, p. 84). No primeiro caso,

$$\Lambda(1, E_n) = -\Lambda(1, E_n) \implies L(1, E_n) = \frac{\sqrt{N}}{2\pi} \Gamma(1) \Lambda(1, E_n) \stackrel{0}{=} 0.$$

No segundo caso, a equação funcional não nos diz nada, mas pode-se mostrar que (KOBLITZ, 1993, p. 95, Proposição 13)

$$L(1, E_n) = 2 \sum_{m=1}^{\infty} \frac{a_m(E)}{m} e^{-2\pi n / \sqrt{N_{E_n}}}, \quad \text{onde } N_{E_n} = \begin{cases} 32n^2, & \text{se } n \text{ é ímpar} \\ 16n^2, & \text{se } n \text{ é par.} \end{cases}$$

Logo, $L(1, E_n)$ pode ser computado para saber se n é congruente ou não. Porém, é esperado que, neste caso, n não seja congruente: sendo uma família de curvas elípticas com

^[240] Este é o triângulo mais “simples” possível para este número!

root number equidistribuído, e em vista da Conjectura de Goldfeld–Katz–Sarnak (Conjectura 5.1.19), metade das curvas elípticas E_n deveria ter posto 0 (n não é congruente) e a outra metade deveria ter posto 1 (n é congruente). A metade que tem posto 1 seria o caso anterior donde, conjecturalmente, $L(E_n, 1) \neq 0$ para 100% dos $n \equiv 1, 2, 3 \pmod{8}$.

Em suma,

- $n \equiv 1, 2, 3 \pmod{8} \implies L(E_n, 1) \neq 0$ quase sempre (conjecturalmente);
- $n \equiv 5, 6, 7 \pmod{8} \implies L(E_n, 1) = 0$.

Exemplo A.2.5. Para $n = 2020$, o Teorema A.2.2 é inconclusivo. Porém, pelo critério acima, $r_{\text{an}}(E_{2020}) = 0$. Pelo Teorema de Kolyvagin–Rubin (4.3.17), $r_{\text{alg}}(E_{2020}) = 0$, donde 2020 não é um número congruente.

A.2.2 Primos que são somas de dois cubos racionais

Seja p um primo ímpar. Não é possível expressar p como soma de dois cubos inteiros, devido à fatoração

$$A^3 + B^3 = (A + B)(A^2 + B^2 - AB).$$

Porém, é possível expressar p como soma de dois cubos *racionais*?^[241]

Considere a curva elíptica^[242] $E_p: x^3 + y^3 = p$. Perguntar se p se expressa como soma de dois cubos racionais é equivalente a perguntar se E_p possui ponto racional. Tal ponto, pelo comentário acima, não pode ter ambas as coordenadas inteiras. Logo, pelo Teorema de Nagell–Lutz (Teorema 3.3.1), tal ponto deveria ser de ordem infinita. Em suma,

Teorema A.2.6. Um primo $p > 2$ é soma de dois cubos racionais se, e somente se, $r_{\text{alg}}(E_p) > 0$.

Se vale a conjectura BSD, isto é equivalente a $L(1, E_p) = 0$, o que é bem mais fácil de verificar (VILLEGAS; ZAGIER, 1995):

- $p \equiv 2, 3, 5 \pmod{9} \implies L(E_p, 1) \neq 0$;
- $p \equiv 4, 7, 8 \pmod{9} \implies L(E_p, 1) = 0$;
- $p \equiv 1 \pmod{9}$: decidível numericamente:

$$L(E_p, 1) = \frac{\sqrt{3}\Gamma(\frac{1}{3})^3}{2\pi\sqrt[3]{p}} S_p,$$

onde $S_p = 0$ se $r_{\text{alg}}(E_p) > 0$ (obviamente!) e, se $r_{\text{alg}}(E_p) = 0 \iff E_p(\mathbb{Q}) = 0$, S_p é um inteiro que, pela Conjectura forte de Birch e Swinnerton-Dyer, é esperado ser $\#III(E)$.

^[241] $2 = 1^3 + 1^3$ certamente é a soma de dois cubos racionais.

^[242] Note que E_p é um curva plana não-singular de gênero 1. Alternativamente, a mudança de coordenadas $(x', y') = \left(\frac{12p}{x+y}, \frac{36p(x-y)}{x+y}\right)$ coloca E_p na forma $y^2 = x^3 - 432p^2$.

A.3 Linha do tempo da conjectura BSD

Para colocar as coisas em perspectiva, listamos alguns dos principais eventos relacionados à conjectura BSD em ordem cronológica.

- **1929:** (Mordell) O grupo de uma curva elíptica sobre $\mathbb{Q}$ é finitamente gerado. Anos mais tarde, Weil fez o mesmo para variedades abelianas mais gerais;
- **1936:** (Hecke) A L -função de uma autoforma $f \in \mathbb{S}_2(\Gamma_0(N))$ satisfaz uma equação funcional interessante;
- **1951:** (Selmer) Primeira descrição dos posteriormente denominados grupos de Selmer de uma curva elíptica;
- **1956:** Birch e Swinnerton-Dyer, baseados em evidências computacionais, propõem uma relação entre $r_{\text{an}}(E)$ e $r_{\text{alg}}(E)$. Nasce a Conjectura de Birch e Swinnerton-Dyer;
- **1958-59:** Tate e Shafarevich começam a estudar independentemente o grupo $\text{III}(E)$. Conjectura-se sua finitude. A conjectura BSD é refinada, descrevendo o coeficiente líder de $L(s, E)$ em termos de $\#\text{III}(E)$;
- **1962:** (Cassels) Existe um pareamento alternado bilinear em $\text{III}(E)$. Em particular, se $\text{III}(E)$ é finito, este pareamento é não-degenerado e $\#\text{III}(E)$ é um quadrado perfeito;
- **1960s:** (Hasse–Weil) L -funções de curvas elípticas também devem satisfazer equações funcionais interessantes, como as das autoformas de Hecke;
- **1977:** (Coates–Wiles) $r_{\text{an}}(E) = 0 \implies r_{\text{alg}}(E) = 0$, para certas curvas elípticas com multiplicação complexa;
- **1978:** (Mazur) Determinadas as possibilidades para o subgrupo de torção de uma curva elíptica sobre $\mathbb{Q}$;
- **1979:** (Goldfeld) Formalização de uma conjectura “folclórica” para curvas elípticas definidas sobre certos corpos quadráticos: 50% das curvas elípticas têm posto analítico 0, 50% têm posto analítico 1, 0% têm posto analítico maior que 1 (*i.e.* curvas de posto alto são raras);
- **1986:** (Gross–Zagier) $r_{\text{an}}(E) = 0 \implies r_{\text{alg}}(E) = 0$ para toda curva elíptica que satisfizesse a conjectura de Taniyama–Shimura;
- **1989-91:** (Kolyvagin–Rubin) $r_{\text{an}}(E) \leq 1 \implies r_{\text{an}}(E) = r_{\text{alg}}(E)$ e $\text{III}(E)$ é finito;
- **1992:** (Brumer) Assumindo a Conjectura BSD e a Hipótese de Riemann Generalizada (HRG), o posto analítico médio é menor que 2,3;

- **1995:** (Taylor–Wiles) A Conjectura de Taniyama–Shimura é válida para curvas elípticas semi-estáveis (e vale o Último Teorema de Fermat!);
- **1999:** (Katz–Sarnak) Generalização da conjectura de Goldfeld sobre a distribuição do posto para todas as curvas elípticas sobre $\mathbb{Q}$;
- **2001:** (Breuil–Conrad–Diamond–Taylor) A Conjectura de Taniyama–Shimura se torna o Teorema da Modularidade: $L(s, E)$ está definida em $s = 1$;
- **2004-06:** Melhorias na cota superior para o posto algébrico médio (ainda assumindo BSD e HRG): 2 (Heath-Brown) e $25/14$ (Young);
- **2006-09:** (Elkies) Os maiores postos algébricos conhecidos são 19 (exato) e ≥ 28 (exato assumindo HRG);
- **2013:** (Bhargava–Shankar) $1,5$ é uma cota superior para o posto algébrico médio que *independe* de BSD e de HRG. Posteriormente melhorada para $7/6$ e $\approx 0,89$ (primeira cota abaixo de 1). Os novos métodos empregados conferirão a Bhargava a Medalha Fields no ano seguinte;
- **2014:** (Bhargava–Skinner–Zhang) Pelo menos $66,48\%$ das curvas elípticas possuem $r_{\text{an}}(E) = r_{\text{alg}}(E) \leq 1$. Em particular a maioria das curvas elípticas satisfaz a Conjectura de Tate–Shafarevich e a Conjectura BSD!